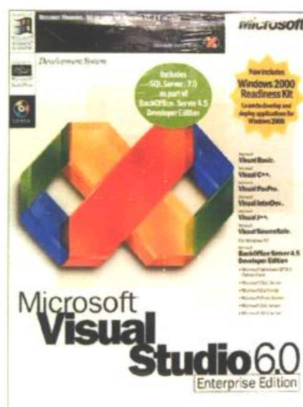
HACK X CRACK: OCULTACIÓN AVANZADA DE FICHEROS

PC PASO a PASO

Iniciamos nuestro curso de VISUAL BASIC

ENGANCHATE !!!

Aprende a PROGRAMAR DESDE CERO :)



ALQUILA UN DVD Y...



CREA UNA COPIA EN CD

TRASTEANDO CON EL HARDWARE DE UNA LAN: ARRIBA LAS MANOS !!!

eMule: LIDER INDISCUTIBLE LAS REDES P2P



COMPARTE TUS PROGRAMAS !!!

TENDENCIAS ACTUALES EN CODIGO MALICIOSO: VIRUS EN EL 2003

Nº 6 -- P.V.P. 4,5 EUROS



HACK X CRACK - HACK X CRACK - HACK X CRACK

HEMOS PUESTO UN SERVIDOR A TU DISPOSICIÓN HACKEANOS !!!

LOS CUADERNOS DE HACK X CRACK

www.hackxcrack.com

FICHEROS STREAM

(INVISIBLES, PELIGROSOS Y EJECUTABLES)

"RIPPEANDO" VIDEOS DIVX ;) EL REY

OCULTACIÓN AVANZADA DE FICHEROS EN WINDOWS XP

eMule programas GRATIS !!!

LISTADO DE PUERTOS Y SERVICIOS: IMPRESCINDIBLE !!!

IPHXC: EL TERCER TROYANO DE HACK X CRACK (PARTE 1)

VIRUS INDETECTABLES 2003 !!! -- OCULTACIÓN EXTREMA



LOS CUADERNOS DE HACK X CRACK
www.hackxcrack.com

EDITORIAL: EDITOTRANS S.L.
C.I.F: B43675701

Director Editorial
I. SENTIS

E-mail contacto
director@editotrans.com

Título de la publicación
Los Cuadernos de HACK X CRACK.

Nombre Comercial de la publicacíón
PC PASO A PASO

Web
www.hackxcrack.com

Deposito legal: B.26805-2002
Código EAN: 8414090202756
Código ISSN: En proceso



Director de la Publicación
J. Sentís

E-mail
director@hackxcrack.com

Diseño gráfico:
J. M. Velasco

Contacto diseñador gráfico
grafico@hackxcrack.com

Redactores
AZIMUT, ROTEADO, FASTIC, MORDEA, FAUSTO, ENTROPIC, MEIDOR, HASHIMUIRA, BACKBONE, ZORTEMIUS, AK22, DORKAN, KMORK, MAILA, TITINA, SIMPSIM... ... ...

Contacto redactores
redactores@hackxcrack.com

Colaboradores
Mas de 130 personas: de España, de Brasil, de Argentina, de Francia, de Alemania de Japón y algún Estadounidense.

Contacto colaboradores
colaboradores@hackxcrack.com

Imprime
I.G. PRINTONE S.A. Tel 91 808 50 15

Distribución
Coedis S.L. Avda. de Barcelona 225. Molins de Rei. Barcelona. Tel 93 680 03 60 FAX 93 668 82 59
WEB: www.coedis.com (mapa de distribución en la web)

NUMERO 5 -- PRINTED IN SPAIN
PERIOCIDAD MENSUAL

DECLARACION DE INTENCIONES

PARA "LOS OTROS":

1.- La intención de la presente publicación NO ES fomentar la piratería informática ni la "delincuencia" en la Red.
2.- Cualquier texto publicado es VALIDADO por nuestra Asesoría Jurídica, por lo que advertimos a cualquier persona, empresa u organización de la inutilidad de cualquier iniciativa jurídica en nuestra contra. Aun así, en caso de cualquier iniciativa en contra de esta revista, deberá ser debidamente presentada y resuelta en la Razón Social que figura en nuestros documentos de constitución.
3.- Esta publicación no se hace responsable del mal uso de los conocimientos que se exponen.
4.- Esta publicación NO FACILITARÁ los datos de nuestros colaboradores ni el origen de nuestros conocimientos salvo ORDEN JUDICIAL y, aun así, advertimos que algunos de esos colaboradores NO SON CONOCIDOS mas que por sus NICKS (alias). Por ello, correrá a cargo de los organismos pertinentes su "descubrimiento".
5.- Esta publicación NO SE HACE RESPONSABLE ni tienen por qué COMPARTIR las opiniones personales vertidas por sus colaboradores, por lo que NO SOMOS RESPONSABLES de las mismas.
6.- Cualquier texto publicado estará bajo las protecciones de DERECHOS DE AUTOR y no se permite su copia, publicación, modificación o distribución sin antes obtener el permiso de esta editorial. De este punto quedan exentos aquellos textos que han sido obtenidos de terceros y/o que están sujetos a otras licencias (ya sean por parte de su autor o por terceros).
7.- Si desean ponerse en contacto con nuestro departamento jurídico, rogamos enviar mail a juridico@hackxcrack.com

PARA NUESTROS LECTORES:

Como podréis ver, esta no es una revista mas, por primera vez tenéis ante vosotros una publicación LIBRE que os ofrecerá la posibilidad de explorar la red tal y como debe explorarse ;)

Esta publicación responde a la pregunta mas veces expuesta en LA RED: ¿Como puedo ser un hacker? Bien, ahora seguro que muchos ya se están "sonriendo" y pensando lo ilusos que somos al intentar "eregirnos" en "portadores de LA LUZ", pensando que seremos una "escuela de lamers" y similares a otras publicaciones que, entre sus 100 páginas de revista solo contiene 5 de "material utilizable" (si es que puede llamarse así).

Pues NO, lo siento, vosotros seréis nuestros jueces y, llegado el caso, NUESTROS VERDUGOS.

Nuestro objetivo es: ACABAR CON LA BASURA DE LA RED (lamers y demás "esencias") con el único método que conocemos: LA EDUCACIÓN y con un única bandera que será por siempre nuestra firma: SOLO EL CONOCIMIENTO TE HACE LIBRE.

Estos son nuestros pilares: LA EDUCACIÓN Y EL CONOCIMIENTO. Para ser un HACKER (maldita palabra mal entendida por unos y peor utilizada por otros) solo hace falta dos cosas: curiosidad y medios, a partir de ahora la curiosidad deberéis ponerla VOSOTROS, porque los medios los facilitaremos NOSOTROS. En las siguientes líneas os descubrimos cómo podremos conseguir nuestros objetivos y definimos algunas de las palabras que más han sido violadas y retorcidas en su significado.

Hacker: Este término ha sufrido a lo largo de su corta historia una horrible conspiración perpetrada por la ignorancia de los medios, eso que personalmente llamo "periodismo de telediario" (en clara alusión a los ridículos artículos que no hacen mas que intoxicar nuestra percepción de las cosas e insultar nuestra inteligencia). Ese tipo de periodismo unido a "otros poderes", desde los monopolios que deben justificar su incompetencia hasta los gobiernos que deben justificar sus intereses ocultos pasando por la industria del cine (normalmente demonológica) y los medios informativos "de masas".

Pues bien, HACKER no es mas que una persona que posee conocimientos avanzados sobre una materia en concreto, normalmente relacionados con la tecnología aunque ni mucho menos limitado a ello. Ponen sus aptitudes al servicio de un único objetivo: EL CONOCIMIENTO. Desean conocer el funcionamiento de "las cosas" y no encuentran límites en sus camino mas que su propia curiosidad. No se dedican a destruir ni a causar estragos entre sus "victimas", no se dedican a robar ni a chantajear ni a regodearse de sus "conquistas", muy al contrario suelen advertir a terceros de las debilidades de sus sistemas y, desgraciadamente, esos "terceros" en lugar de agradecerles su aviso se dedican a denunciarlos o perseguirlos... aunque no siempre es así, por supuesto, muchas compañías y gobiernos han aprendido lo valiosos que son los HACKERS y ahora algunos son colaboradores (o empleados) de estos. **BILL GATES** es un HACKER (el papá ventanas), como **Linus Torvalds** (el papá Linux) o **Grace Hooper** (la Almirante, creadora del Lenguaje COBOL), los autores del COREWAR **Robert Thomas Morris, Douglas McIlroy** y **Victor Vysottsky** (precursores de los creadores de virus informáticos), **Fred Cohen** (el primer investigador y autor de los virus de la historia), **Dennis Ritchie** y **Ken Thompson** ("hacedores" del Lenguaje C y co-creadores del SO UNIX), **Gary Kildall** (autor del sistema operativo CMP y CPM/86), **Tim Paterson** (autor del Quick & Dirty DOS), **Morris** (autor de "The tour of the Worm"), **Kevin Mitnick** (el más buscado por el FBI), **Phiber Optik** (líder juvenil convertido en símbolo de los hackers), **Richard Stallman** (impulsor del "software gratuito" y GNU), **Johan Helsingius** (primer conductor de un Remailer Anónimo), **Chen Ing-Hou** (autor del virus CIH -Chernobyl-), **Sir Dyistic** (creadorutor del Back Orifice), **David L. Smith** (virus Melissa), **Reonel Ramonez** (virus LoveLetter), **Vladimir Levin** (Robó electrónicamente 10 millones de dólares al Citibank), y muchos mas. ¿Cómo? ¿Pero no hemos dicho que los hackers no comenten delitos? Pues NO, vuelve a leer su definición... pero claro, de todo hay en la viña del señor, y al igual que hay delincuentes entre el clero hay hackers que en un momento u otro han ·caido· en la ilegalidad, nadie es perfecto!!!!! ... y **Bill Gates** es un HACKER? Por supuesto, solo tienes que leerte su biografía. ¿Sorprendido? Espero que no, porque eso no es nada mas que un cero a la izquierda en comparación con lo que vas a encontrar en esta revista.

EDITORIAL:
" UNA DE CAL Y OTRA DE ARENA "

El NÚMERO 6 ! Parece mentira que estemos aquí ! Hace muy poquito tiempo, cuando un grupo de "locos" decidió "crear" una revista llamada HACK X CRACK (ahora PC PASO A PASO), creía que con dedicarle al tema 3 ó 4 horas al día sería más que suficiente. QUE INGENUOS !!! Nadie más que nuestros lectores del foro y los que nos han seguido desde el principio saben lo difícil que ha sido mantenernos en "la calle".

El número 6 tenía que ser el número del "asentamiento", cuando pasásemos de los cuadernillos en blanco y negro a una revista en color... pero debido a los problemas que hemos ido contando en cada número tuvimos que dar ese paso en el número 4, junto a un cambio de nombre y formato. Deberíamos estar contentos por "adelantarnos" , pero la realidad ya la conocen nuestros lectores, amigos y colaboradores: fue un cambio forzado por las situaciones, no una transición programada y progresiva.

Así que, aquí estamos sufriendo las consecuencias de las "prisas" y una de ellas ha sido los continuos retrasos en la actualización de la Web. Desde esta editorial pedimos disculpas a nuestros lectores y prometemos que invertiremos más tiempo en la Web de Hack x Crack (www.hackxcrack.com) para que puedas seguir nuestras prácticas sin interrupciones.

Hay algo importante que debo deciros, PC PASO A PASO prepara su "segunda etapa". No nos atrevemos a dar una fecha PERO estamos muy cerca de ampliar la revista en 32 páginas más PORQUE NO PODEMOS SEGUIR ASÍ. No podemos abordar temas que implican, por ejemplo, llenar 20 páginas de RFCs traducidos al castellano y meternos de lleno en 4 ó 5 cursos de programación al mismo tiempo. Así que estamos trabajando para que dentro de poco SEA POSIBLE hacer esas cosas. En esta segunda etapa empezaremos a ver artículos "avanzados" sobre hacking explicados PASO A PASO. Al mismo tiempo estamos trabajando nuestras "relaciones exteriores", ya hemos empezado a exportar a países latinoamericanos e intentaremos traducir al inglés nuestra revista y exportarla a USA ;p

INDICE

PASA TUS PROPIAS PELICULAS A DIVX ;) PARTE I: PREPARANDONOS, HACIENDO EL FRAMESERVING

Alguna vez puede que haya llegado a tus manos alguna película en un CD y te hayas quedado pensando como puede ser eso... Cuando acabes de leer esta serie de artículos, el tema no tendrá ningún misterio para ti. Aprende a pasar los DVD´s a CD´s normales!

1. EMPEZANDO, CONCEPTOS BASICOS

Con este artículo aprenderemos paso a paso a poder hacernos nuestros backups de películas en DVD, pasar el video del viaje de novios que tienes en miniDV a formato avi mas reducido de tamaño, ...

Pare ello vamos a usar el codec DivX;) 5 que se basa en la tecnología del MPEG-4. Te explico, una película en formato digital no deja de ser una agrupación de ceros y unos que están comprimidos para que ocupen menos. Un uno o un cero ocupa un BIT, y cada punto de imagen puede tener distintas profundidades de color, pongamos como ejemplo, 16 BIT. Pues podéis multiplicar 16 por el ancho y alto de la resolución que tengáis puesto en el monitor y sacareis lo que ocuparía una imagen. Además, tendríais que multiplicar todo esto por el numero de imágenes que tenga la película, ... Exacto, impresionante la cifra, necesitarías un disco duro por película. Pues lo que hacen los codecs de video como el DivX es dar un algoritmo de cálculo que reduzca considerablemente esta suma de bits.

El citado MPEG-4 se refiere a un estándar de compresión de video. Se entiende por estándar algo que se genera para que todo el mundo funcione de la misma forma. Si te fijas cuando vas a la ferretería, todas las piezas siguen un estándar, los tornillos pasan de un diámetro de "x" milímetros a "y" milímetros y no encuentras nada entre medias. A la vez, eso mismo lo encuentras en todas las ferreterías. Pues lo mismo, pero con algoritmos compresores.



Con el DivX...

Con el DivX;) 5 conseguiremos recomprimir el video de una película para que ocupe menos espacio sin perder mucha calidad.

Lo primero que vas a hacer es irte a la página de www.divx.com y hacerte con el codec DivX 5.02 versión pro. Te puedes bajar la versión básica, pero esta solo sirve para ver las películas que están comprimidas con DivX. Entre las pro hay dos tipos, la de pago, que obviamente no vamos a coger, y la que además contiene el programa GAIN que hará aparecer un banner cuando naveguemos por Internet. Si os pasáis por el foro de HackXCrack seguramente haya puesto como quitar este banner.

2. FRAMESERVING

Ala! Qué palabro mas raro!, pos si, eso es lo que vas a hacer a continuación, lo que se

conoce como frameserving. De lo que se trata es de preparar la película en DVD para que pueda ser recomprimida con el divx5. Los DVD vienen comprimidos en MPEG-2 ya que soporta sonido multicanal (lo de que tenga muchos idiomas) gracias a codecs de audio (si, como los de video, pero para el audio) de tipo MP3 o AC3.

RIPEAR EL DVD:

Aclaración sobre el MP3: MP3 proviene de MPEG-2 layer 3, esto es, el audio en MP3 pertenece al estándar MPEG-2.

Para poder trabajar con los archivos del DVD vamos a tener que transferirlos a nuestro disco duro (ripearlos), no solo por problemas de velocidad de acceso a un DVD, que no suele superar creo que los 6x, sino también porque estas películas traen una protección para que no puedan ser copiadas.

Para comprobar que existe esta protección, prueba a ver la película en tu ordenador y mientras se esta reproduciendo haz una captura de pantalla con la tecla ImprPant. Vete al Paint y pega la imagen, verás que donde debería estar la escena de la película aparece en negro, esa es parte de la protección.

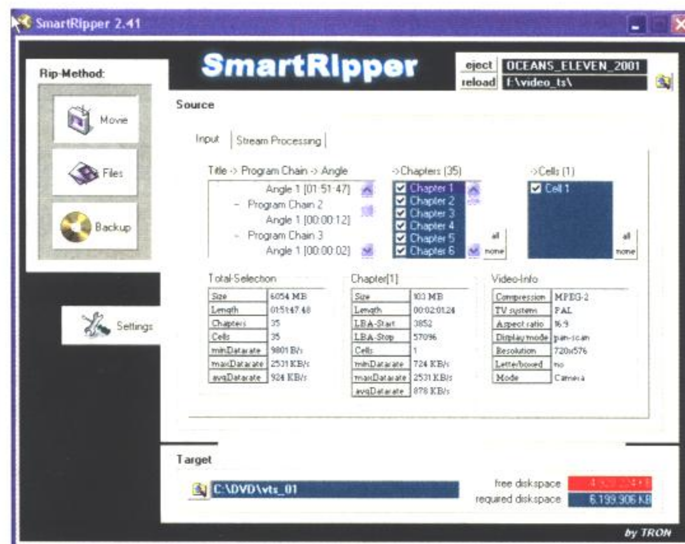


Los DVD vienen...

Los DVD vienen protegidos para que no se puedan utilizar sus contenidos, nos saltaremos esta protección para copiarlos al disco duro.

Si copias los archivos del DVD a tu disco duro directamente, no quitaras esta protección, por lo que vamos a usar algún programa que nos ayude con esto. Mientras buscas el programa que te voy a decir ahora, pon la película a funcionar en segundo plano con el reproductor que mas te guste., esto ayudara a la hora de obtener la protección.

Para poder pasar la película usaremos el SmartRipper, que aunque hay muchos otros, es el que más me gusta XD. Es importante que tengas metidos los últimos ASPI drivers que en estos momentos son: Adaptec ASPI Driver Package 4.72. Nada más ejecutar el Smart Ripper nos encontramos ante esto:





Los drivers aspi...

Los drivers aspi (Advanced SCSI Programming Interface) son utilizados por los programas para comunicarse con los dispositivos SCSI y algunos IDE como lectores y grabadoras. Si tienes problemas al grabar es probable que falten o estén mal instalados.

La verdad es que podríamos explicar este programa en profundidad, pero no lo creo necesario y además, no va a influir mucho en el resultado final. Al arrancarlo, si tenemos ya metido el DVD en la unidad directamente lo carga y selecciona el Title'Program Chain'Angle correspondientes a la película. El resto que aparecen pues corresponderán a los menús y extras que traiga la película. También es frecuente que no haya que modificar nada en las opciones del programa, ya que con las que

se instala por defecto son las que necesitamos.

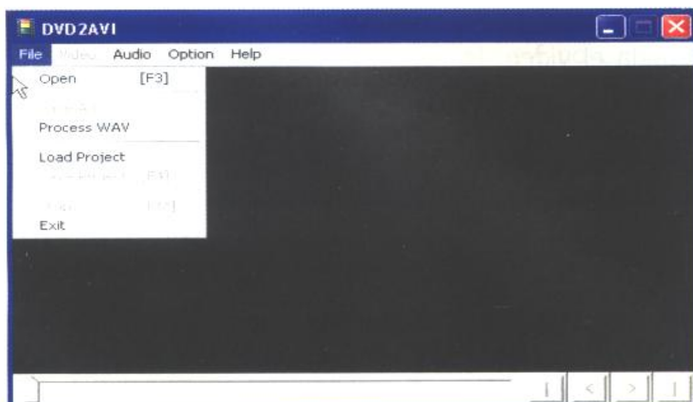
Para comenzar a pasarla al ordenador seleccionaremos en donde pone Target una carpeta de nuestro disco duro, en el ejemplo DVD. A la derecha veis que pone el espacio libre en disco y lo que va a ocupar la película. (En mi caso tengo que vaciar espacio XD). Al haber seleccionado la carpeta os habrá aparecido una opción llamada Stara. Le dais y mientras se copia el DVD os podéis ir a tomar unos chatos.

Cuando haya acabado podéis cerrar el programa e ir a ver lo que ha hecho en vuestro disco duro ;) En la carpeta que seleccionasteis veréis archivos de extensión *.vob que son los que contienen la información de la película, junto con otros. El de más interés para ser visto es el txt que suele tener este nombre: vts_01_INFO.txt

ADAPTANDO EL FORMATO PARA SU PROCESADO:

Bien, de momento hemos conseguido copiar el DVD a nuestro disco duro y quitarle la "protección" que trae. Ahora tenemos que preparar los archivos para poder convertirlos a DivX.

Para esto vamos a usar el DVD2AVI http://arbor.ee.ntu.edu.tw/~jackei/DVD2avi/



Cargamos los archivos del DVD dando a file \ open y seleccionando la carpeta en la que esta el DVD copiado en nuestro disco duro, es más, para que no haya confusiones, saca el DVD del lector y guárdalo en la caja que no coja polvo. Una vez estés en la carpeta veras los archivos vob. Pues seleccionas el primero de la lista "_1.vob" y le das a abrir. Te llevara a otra ventana en la que veras los nombres de todos los vob y en la que solo tienes que darle a "OK". Verás que la pantalla del DVD2avi se ha redimensionado hasta alcanzar el tamaño de pantalla de la película.

Ahora empieza lo entretenido, no me quiero meter todavía en el tema del audio, ya que eso es según gustos, pero tenemos que tomar una pequeña decisión. Te explico, a continuación vamos a crear un proyecto en el cual separamos el audio de la película para trabajar con el video primero y a continuación con el audio para luego volver a juntarlos.

Con el DVD2avi hay dos formas de sacar el audio, en AC3, que es el sonido de la película tal cual, es decir lo mismo que oyes al reproducir el DVD, o en wav, que ocupa mas espacio en disco pero luego nos será útil si queremos tener el sonido en mp3. Tranquilo, te enteraras de lo que hablo cuando llegue el momento de tratar el audio.

Lo primero que vamos a hacer es abrir el txt que nos creó el Smart Ripper y mirar en que pista (track) está el audio que nos interesa. Por ejemplo, en una que tengo yo en el PC:

```
***************
* Stream Info *
***************
```

Stream[001] X=[[0xE0] Video PAL 720x576]

Stream[002] X=[[0x80] Audio Español AC3(6Ch) 48kHz]

Stream[003] X=[[0x81] Audio English AC3(6Ch) 48kHz]

Stream[004] X=[[0x20] Subtitle Español]

Stream[005] X=[[0x??] Others]

Está claro que nos quedaremos con la track 1, no?, fíjate bien, de audio solo hay dos pistas, español e inglés, pos bien, la que aparece primero es la de español, así que será la track1.

Volviendo al DVD2avi, en la pestaño audio seleccionamos "Track number ' Track 1"



Podemos sacar...

Podemos sacar el sonido en dos formatos distintos, AC3 o WAV. La decisión la aprenderás a tomar más adelante.

A continuación separo el manual en dos variantes en función del formato de sonido que queramos.

Sonido en AC3:
Este es el más sencillo, te vas a la pestaña Audio'Output method y seleccionas Demux (AC3, MPA, DTS). El resto de parámetros de la pestaña audio no tienes porque hacer nada con ellos. Solo tener cuidado de tener lo de 48khz'44.1khz en off y el normalization sin seleccionar.

Sonido en WAV:
Vamos a ello. Sacar el sonido en wav es algo mas laborioso pero una vez lo has hecho, te resultara sencillo. Nos vamos a Audio'Output Method y seleccionamos Decode to Wav (AC3, LPCM). Acabamos de seleccionar que queremos que saque el sonido en wav.
A continuación en Audio'Dolby Digital Decode vamos a ver las opciones que ponemos.
Dinamic Range Control: Esta opción se encarga de amplificar mas los sonidos bajos que los altos, para hacer que se oiga mejor si no se dispone de un sistema home cinema de altavoces. En muchas ocasiones no se nota la diferencia cojas la opción que cojas, así que por si acaso, seleccionamos normal.
Dolby Surround Downmix: Esta es otra forma de stereo distinta del convencional. Como no me voy a meter en cuestiones técnicas de porque una u otra, sois libres de elegir lo que queráis. Si seleccionas Downmix pos muy bien y sino también. Probad con distintas películas si queréis.
Pre-Scale Decisión: Esta es una opción muy importante!. Aunque tarde un poco en hacerse es muy importante hacerla. De lo que se encarga es de hacer una primera pasada por el audio estudiando las variaciones de tonos y los picos de volumen y esas cosas. Esto va a afectar a la decodificación del audio, y recomiendo encarecidamente que lo hagáis.

Ya queda menos..., en la sección Audio'48->44.1khz, lo dejamos en off. Aunque si tienes pensado hacer un videocd lo tienes que activar... pero de eso ya hablaremos otro día.

Por último, no del todo, en Normalization seleccionamos entorno a un 90% y lo dejamos activado.

Bien, ya tenemos el audio configurado... nos queda el video. Marcaremos las siguientes opciones. No las voy a explicar tan en profundidad como el sonido ya que son temas algo más complicados y que nos distraerían de lo que realmente estamos haciendo.

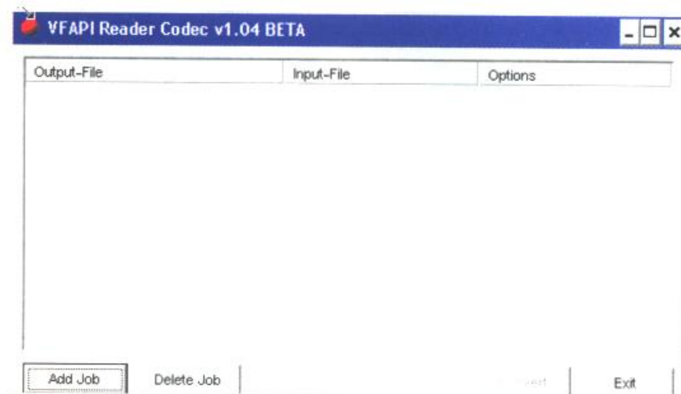
iDCT Algorithm ' 32.bit SSE MMX
Field operation ' None
Color Space ' RGB (rgb corresponde a que esté en color y yuv se utilizaría para películas antiguas en blanco y

negro),
YUV-RGB , pos pc scale
Luminance Filter: Con la barra de desplazamiento de abajo coloca la película en una escena que sea particularmente oscura. Ahora en la pantalla de luminance filter le das al recuadrito y aparecerá un tick. Ahora mueve las barras de Gamma y offset hasta que tengas la imagen a tu gusto, que se vea. En general no hay que poner mas que 6 y 3, pero va en gustos.
La opción clip and resize no la tocaremos, ya que esto lo haremos mas adelante.

Ya lo tenemos todo configurado. Ahora nos vamos al menú File y Save Project. Guardaremos el proyecto con un nombre que queramos, por ejemplo una abreviatura del nombre de la película. Y de nuevo nos iremos por ahí, pero esta vez no de chatos que acabas borracho...

Cuando haya acabado habrás obtenido el audio en el formato que hayas elegido y un archivo de extensión d2v con el nombre que le dieras.

Ahora vamos a necesitar los VFAPI Reader Codec. Este pequeño programa creará a partir del proyecto que acabamos de hacer un archivo de extensión avi. Este avi no será mas que una especie de acceso directo para que se pueda acceder a los archivos vob que contienen la película. Este avi no contiene en ningún caso la película. Simplemente se usa para facilitar el acceso a los vob. Cuando descargues el vfapi, lo primero que deberás hacer es ir a la carpeta codec de donde lo hayas descomprimido y ejecutar vifpset.bat que instalará los codecs. A continuación, en la carpeta Reader ejecutaremos el VFAPIConv-EN.exe y veremos una imagen como esta:



A continuación pulsamos sobre Add Job y seleccionamos el archivo d2v que creamos antes con el DVD2avi. En la siguiente pantalla tendremos que tener seleccionadas todas las opciones (video output y video output by VFAPI reader codec), le damos a OK y en unos segundo se habrá creado ya nuestro pseudo-avi.



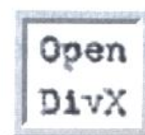
No puedes...

No puedes borrar los archivos del DVD de tu disco duro hasta que no hayamos acabado de recomprimirlos con el DivX. El VFAPI solo crea un pseudo-avi que facilita el acceso a los archivos vob.

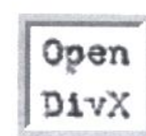
Hasta aquí llega toda la parte del frameserving. Los archivos del DVD ya están listos para ser pasados al formato DivX.











PASA TUS PROPIAS PELICULAS A DIVX;)

PARTE II: RECOMPRESION A DIVX

Hasta ahora hemos conseguido preparar los archivos de un DVD para poder recomprimirlos. Ya va siendo hora de conseguir un archivo que contenga el video y que ocupe el tamaño idóneo para meterlo en uno o dos CD´s.

1. PROGRAMAS NECESARIOS

Lo primero que necesitamos para poder recomprimir el video es tener los programas adecuados que nos ayuden a hacerlo. Os voy a presentar el maravilloso VirtualDub, una joya en su género. Lo podréis conseguir en http://www.virtualdub.org/index os metéis en la sección download y descargáis el archivo llamado "V1.4.13 release build (VirtualDub-1_4_13.zip, 688K zip file)". Si además tienes la suerte de contar con un pentiun IV te bajas el "V1.4.13 executable only, P4 optimized (VirtualDub-1_4_13-P4.zip, 536K zip file)". Además, para los curiosos y amantes de la programación, os podéis bajar el source code que es el código del programa, para que te lo compiles tú mismo, cosa que si supiera os haría hacer... y mucha otra información sobre como esta hecho. Lo dicho, la joya de la corona, te lo dan todo!

Cuando lleguemos a la sección de audio hablaremos un poco sobre los diferentes mods que han hecho del virtualdub gente que no contenta con que solo admita unos pocos formatos de audio quisieron mejorar el programa.

También vamos a necesitar un programa que nos calcule el bitrate (ya lo explico más adelante cuando llegue el momento). En mi opinión el mejor es el Adv. DivX Bitrate Calculador desarrollado por un ruso llamado Mick Thunder y que podréis encontrar en http://DVDrip.nm.ru/

Que no os preocupe no saber ruso, seguro que acertáis a bajároslo, y cuando lo hagáis, podréis ponerlo en inglés. No pensarías que os iba a recomendar un programa del que no entendierais ni papa. XD

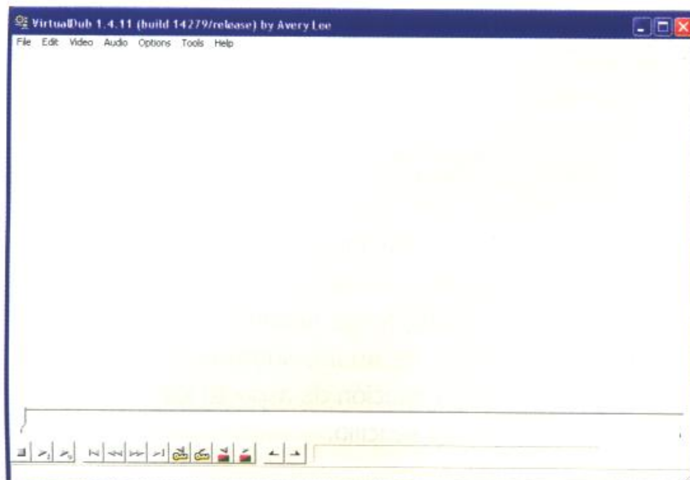
2. CONFIGURANDOLO TODO

Una vez hayáis descargado el VirtualDub tendréis que descomprimirlo y ejecutar el archivo llamado AuxSetup.exe, os aparecerá esto:



Pulsareis sobre Install Handler, para que instale las dll necesarias, y le dais a exit. De esta forma ya estará completamente instalado el vdub (virtualdub, pero pa acortar vdub XD, por si lo repito y alguien se pierde).

Pues, venga, vamos a ejecutar el vdub, podéis emocionaros ;). VirtualDub.exe



Ahora mismo debes de estar pensando que te estoy timando, que un programa a simple vista tan simple no puede ser tan bueno, ya verás ya...

Nos dirigimos a File ' Open video file. Seleccionaremos el archivo .avi que creamos con el vfapi cuando hicimos el frameserving. Que no te has enterado??, reléete lo del frameserving anda... me refiero a aquel pseudo-avi que facilitaba el acceso a los archivos del DVD que tienes en tu disco duro. Le das a "abrir" y se cargará el archivo.

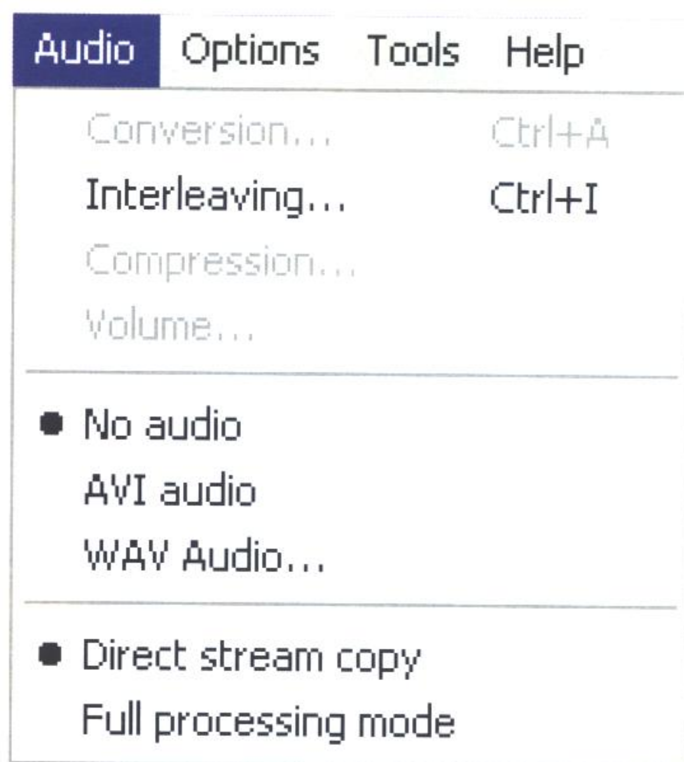
Ahora empieza lo entretenido... al principio te puedes liar, pero una vez que aprendes... lo repites sin pensarlo.

Como bien sabes (o deberías), ahora solo nos estamos encargando del video, para nada del audio, por lo que nos vamos a la pestaña Audio y seleccionamos NO AUDIO.



Es muy importante...

Es muy importante que selecciones No Audio



Bien, de momento ya nos podemos olvidar de la pestaña de audio y no volver a tocarla.

A la hora de pasar una película a DivX hay dos términos que van a tener que ser sobradamente conocidos y que se refieren a dos pasos muy importantes. Son el resize y el cropping.

Comenzaremos explicando el resize. Los DVD suelen venir con un tamaño de imagen de 720*576 píxeles que contiene la escena y las bandas negras míticas que aparecen al ver la película. Pues bien, este tamaño de imagen es excesivo, y utilizarlo conllevaría tener que usar mucho espacio a la hora de hacer la compresión con el DivX. Por ello vamos a modificar el tamaño de la imagen a uno que nos sea más conveniente.

Hasta aquí todo es sencillo de entender. Ahora has de centrarte simplemente en la parte de la imagen que contiene la escena de la película.



Esta imagen guarda siempre una relación de aspecto, es decir, si dividimos el ancho por el alto, siempre guarda una misma relación. Nosotros al hacer el resize tenemos que intentar mantener esa relación en todo lo posible, pero además debemos de cumplir otro par de requisitos, el ancho que pongamos en el resize debe ser un múltiplo de 32, y el del alto debe ser múltiplo de 16.

Así que en resumen, debemos dar un valor X múltiplo de 32 y un valor Y múltiplo de 16, y que además al dividir X entre Y nos de un valor aproximado al de la relación de aspecto de la película. Parece difícil, pero os lo voy a facilitar muchísimo.

1:2.35 --> 640x272, 576x248
1:1.85 --> 640x352, 576x320
1:1.66 --> 640x384, 576x352
1:1.33 --> 640x480, 576x432

En primer lugar están las cuatro relaciones de las que os hablaba y a continuación las resoluciones que podemos poner para cada una. En mi opinión es mejor usar las de 640, pero si queréis podéis usar las de 576, según gustos.

Ahora mismo te estas preguntando como narices vas a saber tu la relación de aspecto que tiene tu película. Hay dos métodos, el primero es el más artesano, reproduces la película a pantalla completa, sacas una regla, mides el ancho de la imagen de la escena, lo divides entre el alto y ves a que valor se asemeja más de los que te he puesto. El segundo método es más elegante aunque menos entretenido... te coges la caja del DVD, le das la vuelta y por donde pone los tipos de audio, subtítulos y demás, encontrarás la relación de aspecto XD, si es que nos lo ponen sencillo.



Resize significa...

Resize significa cambiar el tamaño de la imagen.

Ahora vamos con el cropping. Esto consiste en eliminar las bandas negras que aparece a los lados de las imágenes. Como entenderéis, no queremos gastar espacio recomprimiendo también las bandas negras que total no sirven para nada. A la hora de reproducir la película, gracias a que al hacer el resize tomaremos los múltiplos de 32 y 16, el reproductor que usemos ya nos pondrá las bandas negras.

Ahora os doy la razón por la que prefiero las resoluciones de 640. Si a la imagen inicial de 720*576 le quitamos las bandas negras... nos quedara algo más cercano a 640 el cuadro de la escena... con lo que al elegir las resoluciones de 640 estamos haciendo una imagen más parecida a la del DVD original.



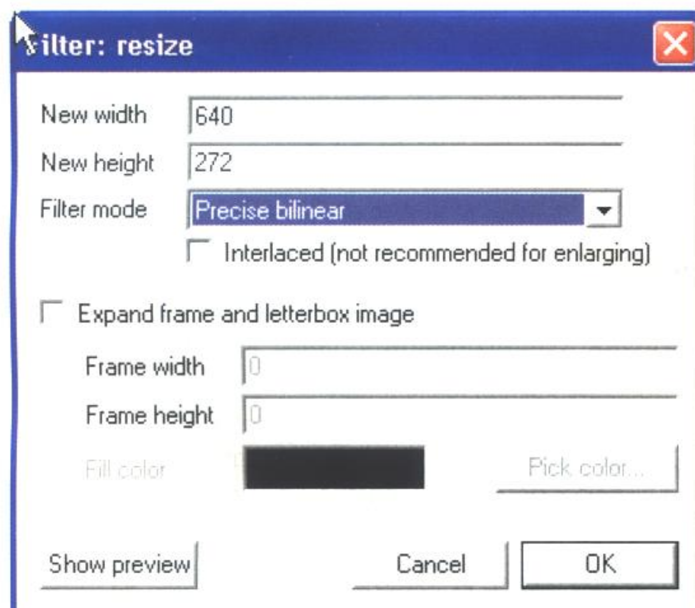
Cropping significa...

Cropping significa recortar cualquier parte de la imagen, en este caso recortar las bandas negras de la imagen hasta quedarnos solo con la escena

Una vez explicados estos dos términos vamos a poner en práctica lo aprendido. Nos vamos al menú video y seleccionamos la opción Filters.

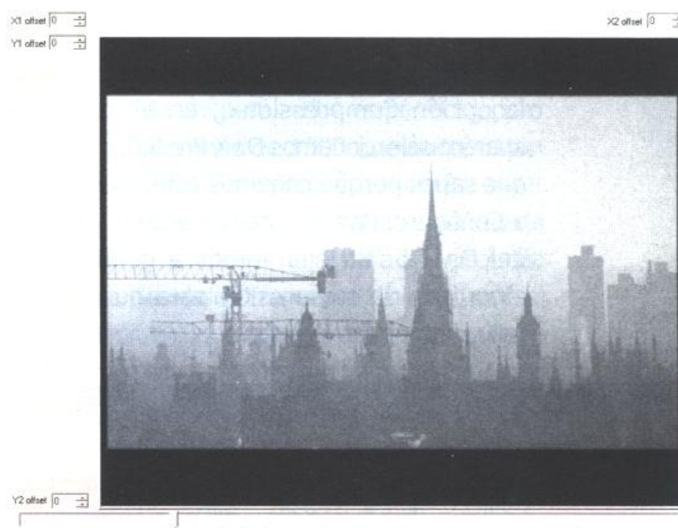


Pulsamos sobre Add... y de la lista seleccionamos el filtro Resize



Te recomiendo que tengas un papel y un boli cerca para que vayas apuntado lo que eliges. En la ventana que aparece al seleccionar el filtro resize introduces la nueva resolución que has elegido (apúntatela). Y en Filter Mode seleccionas Precise Bilinear, esto de momento no influye, luego te explico. Le das a OK y volverás a la pantalla de antes solo que añadido el filtro de resize.

Ahora pulsa sobre Cropping. Te aparcera una nueva ventana en la cual puedes ver imágenes de la película. Con la barra de desplazamiento sitúate en una imagen en la que la escena sea especialmente luminosa, sobre todo en los bordes.



Ahora donde aparece X1, X2, Y1, Y2 ve aumentando el valor hasta que veas que "comes" las bandas negras hasta ajustarlo a la escena. Apúntate los valores que tienes al final poniéndolos según el lado al que correspondan, por ejemplo, con X1 comes banda negra por la izquierda, pos apuntas que el valor corresponde al lado izquierdo, y así con todos.

Ahora pulsas OK y vuelves a la ventana de filters. Ahora teniendo seleccionado el filtro que añadiste, dale a Delete, si, en efecto, bórralo, sin miedo. Lo único que nos interesaba era saber los valores de cropping, que supongo como te he dicho, habrás apuntado. Ahora, viendo que no hay ningún filtro puesto, le das a OK y vuelves al principio del todo.

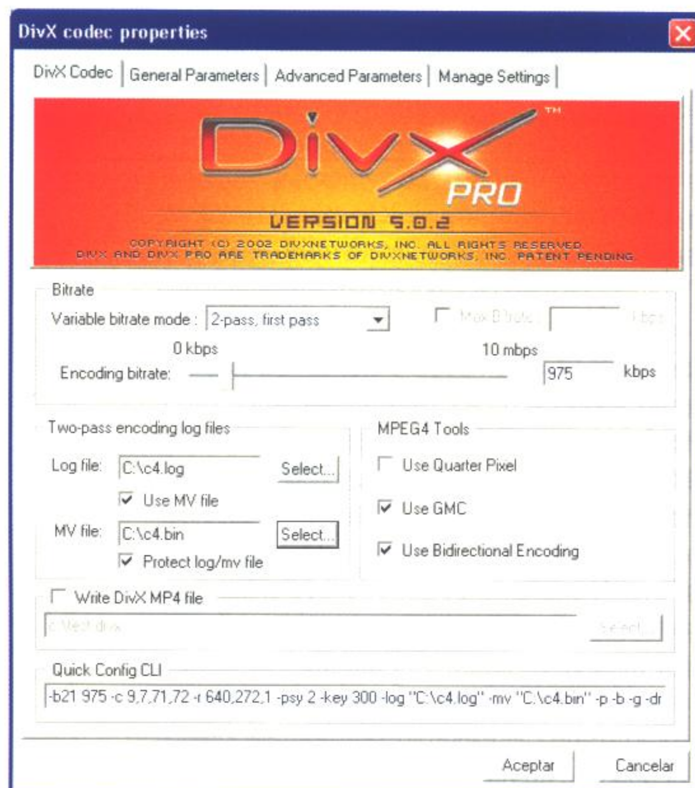


Lo que hemos...

Lo que hemos hecho hasta ahora ha sido para conseguir los valores numéricos del cropping.

Ahora en la pestaña video seleccionas Fast Recompress. Si vuelves a entrar en la pestaña video verás que se han perdido varias opciones, entre ellas las de filters. Utilizamos esta opción de Fast Recompress porque es la mas rápida y ya de por si va a llevar sus horas recomprimir el video en DivX.

Volvemos a la pestaña Video y seleccionamos la opción Compression..., en el menú que aparece seleccionamos DivX Pro 5.0.2, supongo que sabes porque cogemos este... y le damos a Configure. Por fin estamos ante la ventanita del DivX 5. En ella vamos a configurar el algoritmo de compresión para que haga la película a nuestro gusto.



Lo primero que vemos en esta ventana es que nos pide que elijamos el Bitrate. El bitrate es aproximadamente lo que marca el espacio que va a utilizar para cada escena. Cuanto mayor sea el bitrate mayor será el archivo de video que obtendremos y viceversa.



A Bitrate...

A Bitrate más alto, archivo de video más grande, y viceversa.

El DivX nos ofrece tres posibilidades para hacer la compresión:

*1-Pass: Hará la compresión de una sola pasada, ciñéndose en todo lo posible al valor del bitrate que hayamos introducido. En esta opción dedicará más espacio a las escenas con mucho movimiento, donde se suceden más rápidamente escenas muy distintas, y menos a las escenas que son más estáticas.

*1-Pass quality bassed mode: En este caso también hace la compresión de una sola pasada, pero utilizando el bitrate que pusimos sin fijarse en el tipo de escena que tengamos.

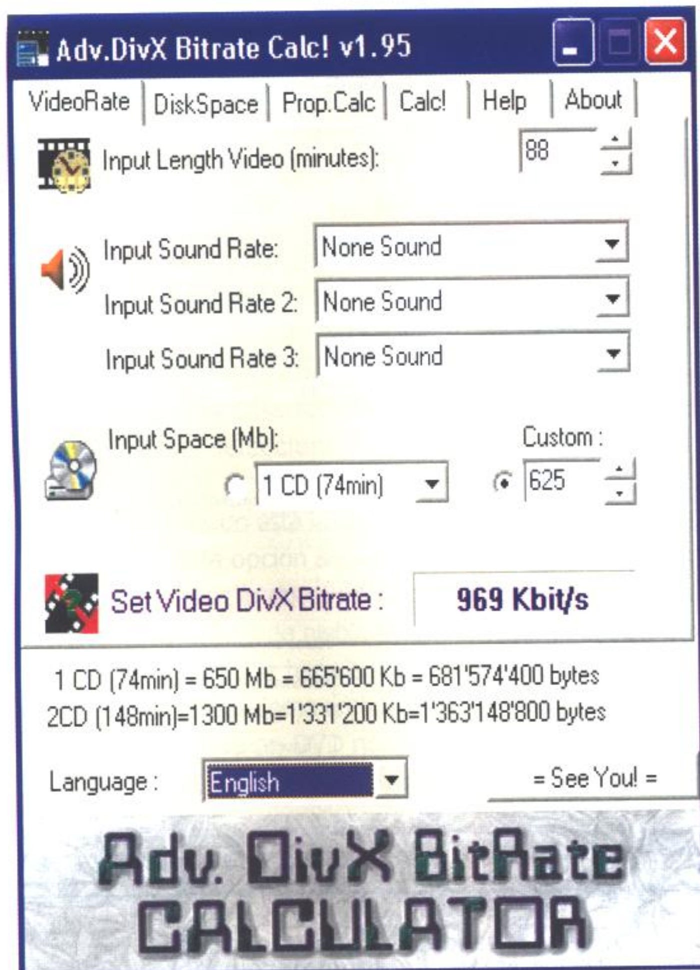
*2-pass: Esté será el modo que utilizaremos. El DivX necesitará hacer dos pasadas para comprimir la película. En la primera comprobara todas las escenas de la película comprobando cuales son los momentos de mayor movimiento, cuales en los que la imagen está prácticamente parada y comprobará la complejidad de la imagen, en función de si tiene mucha variedad de objetos y por tanto es muy compleja, o simplemente es un fondo negro, por ejemplo.



Usaremos el...

Usaremos el modo 2-pass porque optimiza el uso del espacio del archivo de video..

De momento elegimos "2-pass, first pass". Ahora nos toca elegir el bitrate. Para ello usaremos el Advanced DivX Bitrate Calculator.



Hay dos formas de obtener el bitrate, la primera es en la pestaña VideoRate, en la cual introducimos primero el tiempo que dura la película y a continuación la calidad del audio que vamos a utilizar. Luego puedes elegir entre decirle que vas a usar uno de esos formatos de CD que te indica, o decirle que quieres que ocupe X espacio. El segundo método es irte a Disk Space e introducir el tiempo que dura la película, la calidad de sonido que vas a usar e ir poniendo bitrates hasta alcanzar el espacio que deseas.

En mi opinión la mejor forma de hacerlo es teniendo el archivo de audio primero (lo se, todavía no sabes como lo vas a hacer... pero lo aprenderás algún día XD). Una vez sabes lo que ocupa el archivo de audio, le restas este espacio al tamaño del CD que vayas a usar. Ejemplo, si tengo un archivo de sonido que ocupa 70 megas y voy a usar un CD de los de 700, 700-70=630, con lo cual calcularé el bitrate diciéndole que quiero que la película ocupe unos 630 megas. También puedes pensar en hacer las películas en dos CD´s, con lo cual podrás tener mejor calidad de video.

El bitrate aceptable está entre los 850 y los 1000, de ahí para arriba es perfecto, pero nunca busques más de 1300 que no se notan mejorías. Con la práctica aprenderás a ver cuando una película merece la pena o no tenerla en dos CD´s, de momento te daré una pequeña guía para decidirlo. Empezaré diciendo que el valor del bitrate que te da el programa no tiene porque ser exactamente el que necesitas, esto funcionaba bien con DivX anteriores, pero con las mejoras del 5 a veces hasta he subido en 200 la cantidad que me daba el bitrate calculator y obtuve un fichero del tamaño que quería. Esto dependerá de la película.

Lo primero que tienes que tener en cuenta es la duración. A partir de los 110 minutos es razonablemente mejor usar dos CD´s en vez de uno para tener buena calidad de video. Por otra parte tienes que darte cuenta del tipo de película. Por ejemplo, una película de 120 minutos que sea una romanticota, sin mucha acción ni nada, pos en un solo CD seguramente quede bien. Pero si intentas meter una de 100 minutos que se pasen el tiempo corriendo en coches y pegando tiros en un solo CD, seguramente tendrás que perder mucha calidad para conseguirlo.

En la casilla de Encoding Bitrate pon el que obtuviste del programa, con la experiencia aprenderás a variar este número según lo que te interese.

Debajo tenemos la parte de Two-Pass encoding log files, tendrás que seleccionar una carpeta donde guardar un archivo *.log en el primer recuadro y un *.bin en el segundo. En estos

archivos es donde guardará la información que recopile en la primera pasada.

En la pantalla de MPEG-4 tools tenemos tres opciones:

*Use Quarter Píxel: Esto permite que la transición entre escenas o interpolación en el movimiento, se realice por cada cuarto de píxel en vez de cada medio píxel, lo cual hará que tengamos escenas más nítidas en movimientos muy lentos o muy rápidos.

*Use GMC: GMC=Global Motion Compensation, ayuda a mejorar la transición entre imágenes en las que hay un movimiento de toda la escena.

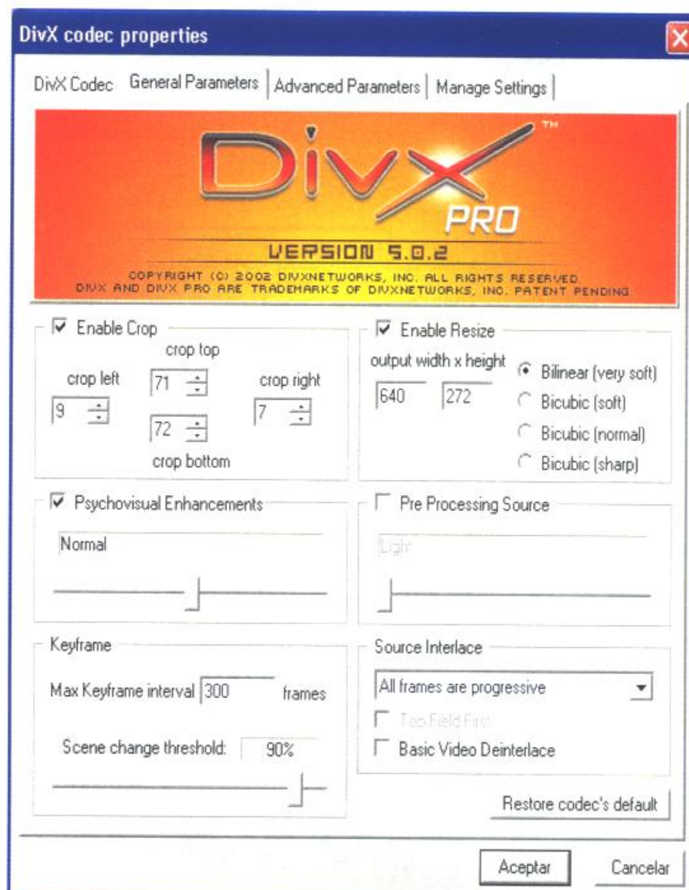
*Use bidirectional encoding: Esta opción facilita la reproducción hacía atrás de los videos, por ejemplo, si queremos volver a un punto en el que nos hemos perdido.

En mi caso solo uso las dos últimas ya que con la primera nunca he notado mucha diferencia y hay que tener en cuenta que cuantas más opciones de estas elijamos, más tiempo tardará en recomprimirse el video.

Debajo viene una opción para convertir nuestros archivos avi en divx4 al estándar de video MPEG-4 el cual tengo entendido que funciona bien para gente que tenga ordenadores poco potentes. Esta opción de momento la ignoraremos.

En la línea inferior aparecen las opciones que estamos modificando desde el entorno gráfico del codec DivX. Sería la secuencia de parámetros que tendríamos que añadir al comprimir desde una pantalla MS-DOS.

Ya por fin podemos pasar a la siguiente pestaña XD, General Parameters



En primer lugar tendremos que seleccionar Enable cropping e introducir los números aquellos que te mande apuntar que se usan para quitar las bandas negras. El hacer el cropping en el codec y no en los filters hace que la recompresión sea más rápida, lo cual será muy importante.

También tendremos que seleccionar la opción de Enable Resize y poner los valores de ancho y alto que determinamos anteriormente. Además tendremos que seleccionar el tipo de resize que queremos usar. En nuestro caso tendremos que usar Bilinear, ya que queremos que la imagen tenga un tamaño inferior a la original. Si por el contrario quisiéramos hacer una imagen mayor que la original tendríamos que seleccionar el bicúbico, aumentando de soft hasta sharp cuanto mayor sea la diferencia entre las dimensiones.



Espero que...

Espero que recordaras apuntar los datos del cropping y el resize.

A continuación tenemos los Psychovisual Enhacements. Estos se basan en engañar al ojo humano para hacerle creer que la imagen es mejor de lo que en realidad es. No está muy desarrollado aunque os recomiendo que lo seleccionéis y lo pongáis en Normal.

Al lado está la opción de Pre Processing Source, esta opción se utiliza cuando el video original tiene lo que se denomina ruido... es decir, una especie de niebla por así decirlo. Es decir, tiene algo que hace que la imagen no sea del todo nítida. Como en nuestro caso estamos pasando desde un DVD no tenemos este problema así que no seleccionaremos esta opción.

Ahora seleccionaremos los Keyframes. Estos frames (escenas) son especiales por una sencilla razón, cuando avances con la barra de desplazamiento al ver el video en un reproductor, estos son los frames en los que se puede parar al soltar la barra, nunca conseguirás dejar la imagen con la barrita esa entre dos escenas de estas (keyframes). Además, los keyframes son las pocas imágenes que se almacenan completas en el archivo de video, las que hay entre ellas solo guardan la modificación que va habiendo con respecto a las anteriores. Estos keyframes se insertan automáticamente cuando el codec detecte un cambio grande entre escenas, pero además habrá que añadir otros. En el recuadro de Max Keyframes Treshold pondremos el valor de 300, así si cada 300 escenas el codec no metió automáticamente un keyframe, se insertará uno. Este valor en Europa, PAL, donde los videos usan el estándar de 25fps (frames per second) corresponde a un keyframe cada 12 segundos de video. En la barra de Scene change treshold un valor de 90 suele estar bien, ya que con 100% podríamos tener un keyframe por cada frame, lo cual no sería bueno.



Los keyframes...

Los keyframes se almacenan completos, por lo si pones 100% en el treshold seguramente saques un archivo mas grande de lo normal.

Por último, en esta pestaña, nos queda el Source Intelaced. Esto lo usaremos para indicar si el video original viene entrelazado o no. Por lo general los DVD no vienen entrelazados, por lo que seleccionaremos All frames are progressive. Si estuviera entrelazado, tendríamos que seleccionar All frames are interleaced. Sobre como saber si el video esta entrelazado hay muchas discrepancias, sobre todo con los programas que se supone que te lo dicen que no siempre aciertan. Un truco es ver cuando estábamos el DVD2AVI si al avanzar rápidamente con la barra de desplazamiento (cogiendo con el ratón y moviendo) las imágenes que vemos en pantalla son nítidas (no entrelazado) o borrosas (entrelazado). Esto se debe a que en el entrelazado cada imagen tiene guardados simplemen te la mitad de los pixels, y junto con la siguiente se complementan para dar la imagen completa. La opción de Basic video deinterlaced



El tema de...

El tema de entrelazado no está muy bien explicado, pero es porque si me pongo a hablar del entrelazado el texto se puede hacer largísimo y seguramente eterno para muchos

Bueno, ya podemos pasar a la pestaña de Advanced Parameters:



En esta pestaña no tendremos porque cambiar nada, los valores que trae por defecto son los óptimos según los creadores del DivX 5. No obstante, comentaremos un poco por alto las opciones. No pretendo en ningún momento dejar clara totalmente esta parte, ya que son conceptos muy técnicos que a la gente en general no les interesaran para nada.

Primero nos fijaremos en Data Rate Control (RC). Estos valores afectan a la calidad y la precisión con la que trate el codec las diferentes imágenes.

*Maximun and minimun quantizer: Modifican la precisión del codec. Cuanto mayor sea el quantizer, peor será la calidad de cada frame, y viceversa. Seleccionaremos el máximo y el mínimo, y el codec utilizará los quantizer entre esos rangos. El máximo podéis cambiarlo de 12 que viene por defecto a 8. Esto hará un archivo algo mayor, pero que hará tener mayor calidad de imagen. Además, con el divx5, gracias a su gran calidad de compresión, merece la pena ponerlo en 8, ya que los archivos no se agrandarán mucho. El mínimo yo siempre lo tengo puesto en 2 que es el recomendado para películas de acción.

*RC averaging period, frames: Determina el número de frames entorno al que está comprimiendo comprueba, para determinar el mejor bitrate para este frame. Es decir, para ir compensando el bitrate y ajustarse al indicado. Ponerlo en 2000 está bastante bien.

*RC reacting period, frames: Determina lo rápido que reaccionará el codec ante cambios bruscos en el movimiento de las escenas. Con un valor de 10 valdrá.

*Rate control down/up reaction: Determina la sensibilidad del codec a los cambios de velocidad de las escenas. Lo tendremos en 20.

A su derecha encontramos el Data partitioning, que no utilizaremos. En performance quality seleccionaremos slowest. Esto índica el tiempo que dedica el codec a comprimir cada imagen, y cuanto más lento, mejor lo hará.

El apartado de DivX MP4 creator lo dejaremos sin tocar ya que no pretendemos hacer un archivo de este tipo.



Si te interesa...

Si te interesa saber más sobre los valores de la pestaña Advanced parameters, dirígete a la página de DivX o busca información por la red.

Ya por último pasamos a la pestaña de Manage settings, aquí podremos guardar la configuración para cada película que hagamos, así si tenemos que volver a usarla, no hace falta volver a empezar desde cero. Supongo que esta parte no necesita explicación, si alguien la necesita que pase por el foro que seguro que otra

persona se la explica fácilmente.

Pues bien, ya le puedes dar a Aceptar. Volverás a la pantalla de Select Video compression, le das a OK y vuelves por fin al virtualdub con el que empezaste, pero ya configurado.

Bien, hagamos un pequeño repaso, tenemos puesto en la pestaña de Audio la opción de No audio, en la pestaña video ya hemos configurado la compresión, configurando el codec DivX, y además tenemos seleccionada la opción de fast recompress. Pos entonces ya podemos irnos a la pestaña File y darle a Save as avi...

Se te abrirá una ventana donde seleccionaras un nombre para este archivo avi que vas a crear. Te recuerdo que de momento hemos configurado la primera pasada, así que mejor lo llamas con algo acabado en *_1.avi o algo así, que te indique que es el de la primera. Antes de darle a OK seleccionas la opción de Add operation to job list, esto hará que se añada a la lista de tareas del virtualdub el hacer la primera pasada. Le das a OK y vuelves a la ventana del virtualdub.

Ahora, sin haber tocado nada todavía, vamos a configurar la segunda pasada. Te metes otra vez en Video\Compression...\DivX Pro 5.0.2 Codec\ y de nuevo ante la ventana del codec donde antes seleccionaste 2-pass, first pass ahora cambiaras a 2-pass, second pass. Le das a Aceptar y repites la operación para crear el avi, esto es, nos vamos a File\Save as avi...\ pero esta vez seleccionas el nombre acabándolo por ejemplo en *_2.avi y también le das a Add operation to job list.

Bien, ahora solo nos queda poner en funcionamiento la lista de tareas. Al haber preparado las dos pasadas de esta forma las hará del tirón, es decir, cuando acabe una empieza con la siguiente. Nos vamos File\Job Control...\ y en la ventana que aparece le damos a start. De esta forma comenzará la recompresión a DivX del video.

En la ventana del virtual dub puedes hacer que aparezca la Status window en la cual te pondrá el tiempo estimado para que acabe de hacer la pasada que esté haciendo en ese momento. Además podrás seleccionar el nivel de prioridad que tenga el programa, para indicarle cuantos recursos de la cpu puede coger.

De esta forma conseguiremos en archivo _2.avi el video de la película. Eso si, tras varias horas de tener el ordenador haciendo las pasadas, ah cierto, se me olvidaba, jeje. En mi ordenador a 866 mhz tardo unas 4 horas por pasada para hacer una película de 100 minutos. A mas mhz, menos tiempo, aquellos que tengan PIV a 2'no se cuantos mhz, no tendrán problemas de tiempo, seguro....

Ya, ya se que ahora piensas en todo el tiempo que te he dejao sin pc, pero es que si te hubiera dicho al principio lo que ibas a tardar, igual no te hubieras leído el texto y de esta forma, aunque ahora lo mandes a la mierda y digas que pasas de tener el pc trabajando tanto tiempo, al menos habrás aprendido algo XD.

Espero que os guste el cine mudo porque el tema del Audio será pal número que viene. Espero que ya habreis hecho los deberes XD. Sinó, ya podeis tirar el equipo a la basura y comprar uno nuevo.



Nota de la redacción...

Nota de la redacción:

-VirtualDub es uno de los mejores procesadores de video del mercado, siendo gratuito.

PUERTOS Y SERVICIOS

SERVICIOS:

Aquí os presentamos un listado de **Puertos** y **Servicios** extraido directamente de Linux.

La lista tiene el siguiente formato: **Nombre del servicio**, Puerto/Protocolo, Función, #Comentario.

/etc/services:
$Id: services,v 1.4 1997/05/20 19:41:21 tobias Exp $
#
Network services, Internet style
#
Note that it is presently the policy of IANA to assign a single well-known
port number for both TCP and UDP; hence, most entries here have two entries
even if the protocol doesn't support UDP operations.
Updated from RFC 1700, ``Assigned Numbers" (October 1994). Not all ports
are included, only the more common ones.

tcpmux 1/tcp # TCP port service multiplexer
echo 7/tcp
echo 7/udp
discard 9/tcp sink null
discard 9/udp sink null
systat 11/tcp users
daytime 13/tcp
daytime 13/udp
netstat 15/tcp
qotd 17/tcp quote
msp 18/tcp # message send protocol
msp 18/udp # message send protocol
chargen 19/tcp ttytst source
chargen 19/udp ttytst source
ftp-data 20/tcp
ftp 21/tcp
fsp 21/udp fspd
ssh 22/tcp # SSH Remote Login Protocol
ssh 22/udp # SSH Remote Login Protocol
telnet 23/tcp
24 - private
smtp 25/tcp mail
26 - unassigned
time 37/tcp timserver
time 37/udp timserver
rlp 39/udp resource # resource location
nameserver 42/tcp name # IEN 116
whois 43/tcp nicname
re-mail-ck 50/tcp # Remote Mail Checking Protocol
re-mail-ck 50/udp # Remote Mail Checking Protocol
domain 53/tcp nameserver # name-domain server
domain 53/udp nameserver
mtp 57/tcp # deprecated
bootps 67/tcp # BOOTP server
bootps 67/udp
bootpc 68/tcp # BOOTP client
bootpc 68/udp
tftp 69/udp
gopher 70/tcp # Internet Gopher
gopher 70/udp
rje 77/tcp netrjs
finger 79/tcp
www 80/tcp http # WorldWideWeb HTTP
www 80/udp # HyperText Transfer Protocol
link 87/tcp ttylink
kerberos 88/tcp kerberos5 krb5 kerberos-sec # Kerberos v5
kerberos 88/udp kerberos5 krb5 kerberos-sec # Kerberos v5
supdup 95/tcp
100 - reserved
hostnames 101/tcp hostname # usually from sri-nic
iso-tsap 102/tcp tsap # part of ISODE.
csnet-ns 105/tcp cso-ns # also used by CSO name server
csnet-ns 105/udp cso-ns

unfortunately the poppassd (Eudora) uses a port which has already
been assigned to a different service. We list the poppassd as an
alias here. This should work for programs asking for this service.
(due to a bug in inetd the 3com-tsmux line is disabled)
#3com-tsmux 106/tcp poppassd
#3com-tsmux 106/udp poppassd
rtelnet 107/tcp # Remote Telnet
rtelnet 107/udp
pop2 109/tcp postoffice pop-2 # POP version 2
pop2 109/udp pop-2
pop3 110/tcp pop-3#POP version 3
pop3 110/udp pop-3
sunrpc 111/tcp portmapper # RPC 4.0 portmapper TCP
sunrpc 111/udp portmapper # RPC 4.0 portmapper UDP
auth 113/tcp authentication tap ident
sftp 115/tcp
uucp-path 117/tcp
nntp 119/tcp readnews untp # USENET News Transfer Protocol
ntp 123/tcp
ntp 123/udp # Network Time Protocol
pwdgen 129/tcp # PWDGEN service
pwdgen 129/udp # PWDGEN service
netbios-ns 137/tcp # NETBIOS Name Service
netbios-ns 137/udp
netbios-dgm 138/tcp # NETBIOS Datagram Service
netbios-dgm 138/udp
netbios-ssn 139/tcp # NETBIOS session service
netbios-ssn 139/udp
imap2 143/tcp imap # Interim Mail Access Proto v2
imap2 143/udp imap
snmp 161/udp # Simple Net Mgmt Proto
snmp-trap 162/udp
snmptrap # Traps for SNMP
cmip-man 163/tcp # ISO mgmt over IP (CMOT)
cmip-man 163/udp
cmip-agent 164/tcp
cmip-agent 164/udp
mailq 174/tcp # Mailer transport queue for Zmailer
mailq 174/udp # Mailer transport queue for Zmailer
xdmcp 177/tcp # X Display Mgr. Control Proto
xdmcp 177/udp
nextstep 178/tcp NeXTStep NextStep # NeXTStep window
nextstep 178/udp NeXTStep NextStep # server
bgp 179/tcp # Border Gateway Proto.
bgp 179/udp
prospero 191/tcp # Cliff Neuman's Prospero
prospero 191/udp
irc 194/tcp # Internet Relay Chat
irc 194/udp
smux 199/tcp # SNMP Unix Multiplexer
smux 199/udp
at-rtmp 201/tcp # AppleTalk routing
at-rtmp 201/udp
at-nbp 202/tcp # AppleTalk name binding
at-nbp 202/udp
at-echo 204/tcp # AppleTalk echo
at-echo 204/udp
at-zis 206/tcp # AppleTalk zone information
at-zis 206/udp
qmtp 209/tcp # The Quick Mail Transfer Protocol
qmtp 209/udp # The Quick Mail Transfer Protocol

z3950	210/tcp wais	# NISO Z39.50 database
z3950	210/udp	wais
ipx	213/tcp	# IPX
ipx	213/udp	
imap3	220/tcp	# Interactive Mail Access
imap3	220/udp	# Protocol v3
rpc2portmap	369/tcp	
rpc2portmap	369/udp	# Coda portmapper
codaauth2	370/tcp	
codaauth2	370/udp	# Coda authentication server
ulistserv	372/tcp	# UNIX Listserv
ulistserv	372/udp	
ldap	389/tcp	# Lightweight Directory Access Protocol
ldap	389/udp	# Lightweight Directory Access Protocol
https	443/tcp	# MCom
https	443/udp	# MCom
snpp	444/tcp	# Simple Network Paging Protocol
snpp	444/udp	# Simple Network Paging Protocol
saft	487/tcp	# Simple Asynchronous File Transfer
saft	487/udp	# Simple Asynchronous File Transfer
npmp-local	610/tcp	dqs313_qmaster # npmp-local / DQS
npmp-local	610/udp	dqs313_qmaster # npmp-local / DQS
npmp-gui	611/tcp	dqs313_execd # npmp-gui / DQS
npmp-gui	611/udp	dqs313_execd # npmp-gui / DQS
hmmp-ind	612/tcp	dqs313_intercell # HMMP Indication / DQS
hmmp-ind	612/udp	dqs313_intercell # HMMP Indication /

		DQS
ipp	631/tcp	# Internet Printing Protocol
ipp	631/udp	# Internet Printing Protocol

#
UNIX specific services
#

exec	512/tcp	
biff	512/udp	comsat
login	513/tcp	
who	513/udp	whod
shell	514/tcp	cmd # no passwords used
syslog	514/udp	
printer	515/tcp	spooler # line printer spooler
talk	517/udp	
ntalk	518/udp	
route	520/udp	router routed #RIP
timed	525/udp	timeserver
tempo	526/tcp	newdate
courier	530/tcp	rpc
conference	531/tcp	chat
netnews	532/tcp	readnews
netwall	533/udp	# -for emergency broadcasts
gdomap	538/tcp	# GNUstep distributed objects
gdomap	538/udp	# GNUstep distributed objects
uucp	540/tcp	uucpd # uucp daemon
afpovertcp	548/tcp	# AFP over TCP
afpovertcp	548/udp	# AFP over TCP
remotefs	556/tcp	rfs_server rfs # Brunhoff remote filesystem
klogin	543/tcp	# Kerberized `rlogin' (v5)
kshell	544/tcp	krcmd # Kerberized `rsh' (v5)
nntps	563/tcp	snntp # NNTP over SSL
nntps	563/udp	snntp # NNTP over SSL

ldaps 636/tcp # LDAP over SSL
ldaps 636/udp # LDAP over SSL
tinc 655/tcp # tinc control port
tinc 655/udp # tinc packet port
kerberos-adm 749/tcp # Kerberos `kadmin' (v5)
#
webster 765/tcp # Network dictionary
webster 765/udp
rsync 873/tcp # rsync
rsync 873/udp # rsync
ftps-data 989/tcp # FTP over SSL (data)
ftps 990/tcp # FTP over SSL
telnets 992/tcp # Telnet over SSL
telnets 992/udp # Telnet over SSL
imaps 993/tcp # IMAP over SSL
imaps 993/udp # IMAP over SSL
ircs 994/tcp # IRC over SSL
ircs 994/udp # IRC over SSL
pop3s 995/tcp # POP-3 over SSL
pop3s 995/udp # POP-3 over SSL
#
From ``Assigned Numbers'':
#
#> The Registered Ports are not controlled by the IANA and on most systems
#> can be used by ordinary user processes or programs executed by ordinary
#> users.
#
#> Ports are used in the TCP [45,106] to name the ends of logical
#> connections which carry long term conversations. For the purpose of
#> providing services to unknown callers, a service contact port is
#> defined. This list specifies the port used by the server process as its
#> contact port. While the IANA can not control uses of these ports it
#> does register or list uses of these ports as a convienence to the
#> community.
#
socks 1080/tcp # socks proxy server
socks 1080/udp # socks proxy server
lotusnote 1352/tcp lotusnotes # Lotus Note
lotusnote 1352/udp lotusnotes # Lotus Note
ingreslock 1524/tcp
ingreslock 1524/udp
prospero-np 1525/tcp # Prospero non-privileged
prospero-np 1525/udp
datametrics 1645/tcp old-radius # datametrics / old radius entry
datametrics 1645/udp old-radius # datametrics / old radius entry
sa-msg-port 1646/tcp old-radacct # sa-msg-port / old radacct entry
sa-msg-port 1646/udp old-radacct # sa-msg-port / old radacct entry
radius 1812/tcp # Radius
radius 1812/udp # Radius
radius-acct 1813/tcp radacct # Radius Accounting
radius-acct 1813/udp radacct # Radius Accounting
rtcm-sc104 2101/tcp # RTCM SC-104 IANA 1/29/99
rtcm-sc104 2101/udp # RTCM SC-104 IANA 1/29/99
cvspserver 2401/tcp # CVS client/server operations
cvspserver 2401/udp # CVS client/server operations
venus 2430/tcp # codacon port
venus 2430/udp # Venus callback/wbc interface
venus-se 2431/tcp # tcp side effects
venus-se 2431/udp # udp sftp side effect
codasrv 2432/tcp # not used
codasrv 2432/udp # server port
codasrv-se 2433/tcp # tcp side effects
codasrv-se 2433/udp # udp sftp side effect
mon 2583/tcp # MON

mon 2583/udp # MON
dict 2628/tcp # Dictionary server
dict 2628/udp # Dictionary server
gds_db 3050/tcp # InterBase server
gds_db 3050/udp # InterBase server
icpv2 3130/tcp icp # Internet Cache Protocol (Squid)
icpv2 3130/udp icp # Internet Cache Protocol (Squid)
mysql 3306/tcp # MySQL
mysql 3306/udp # MySQL
rfe 5002/tcp # Radio Free Ethernet
rfe 5002/udp # Actually uses UDP only
cfengine 5308/tcp # CFengine
cfengine 5308/udp # CFengine
x11 6000/tcp x11-0 # X windows system
x11 6000/udp x11-0 # X windows system
x11-1 6001/tcp # X windows system
x11-1 6001/udp # X windows system
x11-2 6002/tcp # X windows system
x11-2 6002/udp # X windows system
x11-3 6003/tcp # X windows system
x11-3 6003/udp # X windows system
x11-4 6004/tcp # X windows system
x11-4 6004/udp # X windows system
x11-5 6005/tcp # X windows system
x11-5 6005/udp # X windows system
x11-6 6006/tcp # X windows system
x11-6 6006/udp # X windows system
x11-7 6007/tcp # X windows system
x11-7 6007/udp # X windows system
afs3-fileserver 7000/tcp bbs # file server itself
afs3-fileserver 7000/udp bbs # file server itself
afs3-callback 7001/tcp # callbacks to cache managers
afs3-callback 7001/udp # callbacks to cache managers
afs3-prserver 7002/tcp# users & groups database
afs3-prserver 7002/udp# users & groups database
afs3-vlserver 7003/tcp # volume location database
afs3-vlserver 7003/udp# volume location database
afs3-kaserver 7004/tcp # AFS/Kerberos authentication
afs3-kaserver 7004/udp# AFS/Kerberos authentication
afs3-volser 7005/tcp # volume managment server
afs3-volser 7005/udp# volume managment server
afs3-errors 7006/tcp # error interpretation service
afs3-errors 7006/udp# error interpretation service
afs3-bos 7007/tcp # basic overseer process
afs3-bos 7007/udp # basic overseer process
afs3-update 7008/tcp # server-to-server updater
afs3-update 7008/udp # server-to-server updater
afs3-rmtsys 7009/tcp # remote cache manager service
afs3-rmtsys 7009/udp # remote cache manager service
font-service 7100/tcp xfs # X Font Service
font-service 7100/udp xfs # X Font Service
wnn6 22273/tcp # wnn6
wnn6 22273/udp # wnn6

The remaining port numbers are not as allocated by IANA.
#
Kerberos (Project Athena/MIT) services
Note that these are for Kerberos v4, and are unofficial. Sites running
v4 should uncomment these and comment out the v5 entries above.
#
kerberos4 750/udp kerberos-iv kdc

Kerberos (server) udp
kerberos4 750/tcp kerberos-iv kdc # Kerberos (server) tcp
kerberos_master 751/udp # Kerberos authentication
kerberos_master 751/tcp # Kerberos authentication
passwd_server 752/udp # Kerberos passwd server
krb_prop 754/tcp # Kerberos slave propagation
krbupdate 760/tcp kreg # Kerberos registration
kpasswd 761/tcp kpwd # Kerberos "passwd"
swat 901/tcp # swat
kpop 1109/tcp # Pop with Kerberos
knetd 2053/tcp # Kerberos de-multiplexor
zephyr-srv 2102/udp # Zephyr server
zephyr-clt 2103/udp # Zephyr serv-hm connection
zephyr-hm 2104/udp # Zephyr hostmanager
eklogin 2105/tcp # Kerberos encrypted rlogin
Hmmm. Are we using Kv4 or Kv5 now? Worrying.
The following is probably Kerberos v5 --- ajt@debian.org (11/02/2000)
kx 2111/tcp # X over Kerberos
#
Unofficial but necessary (for NetBSD) services
#
supfilesrv 871/tcp # SUP server
supfiledbg 1127/tcp # SUP debugging
#
Datagram Delivery Protocol services
#
rtmp 1/ddp # Routing Table Maintenance Protocol
nbp 2/ddp # Name Binding Protocol
echo 4/ddp # AppleTalk Echo Protocol
zip 6/ddp # Zone Information Protocol
#
Services added for the Debian GNU/Linux distribution
#
linuxconf 98/tcp # LinuxConf
poppassd 106/tcp # Eudora
poppassd 106/udp # Eudora
imsp 406/tcp # Interactive Mail Support Protocol
imsp 406/udp # Interactive Mail Support Protocol
ssmtp 465/tcp smtps # SMTP over SSL
nqs 607/tcp # Network Queuing system
moira_db 775/tcp # Moira database
moira_update 777/tcp # Moira update protocol.
moira_ureg 779/udp # Moira user registration.
omirr 808/tcp omirrd # online mirror
omirr 808/udp omirrd # online mirror
customs 1001/tcp # pmake customs server
customs 1001/udp # pmake customs server
rmiregistry 1099/tcp # Java RMI Registry
skkserv 1178/tcp # skk jisho server port
predict 1210/udp # predict -- satellite tracking
rmtcfg 1236/tcp # Gracilis Packeten remote config server
xtel 1313/tcp # french minitel
xtelw 1314/tcp # french minitel
support 1529/tcp # GNATS
sieve 2000/tcp # Sieve mail filter daemon
cfinger 2003/tcp lmtp # GNU Finger / Local Mail Transfer Protocol
ndtp 2010/tcp # Network dictionary transfer protocol
ninstall 2150/tcp # ninstall service
ninstall 2150/udp # ninstall service

zebrasrv	2600/tcp	# zebra service
zebra	2601/tcp	# zebra vty
ripd	2602/tcp	# RIPd vty
ripngd	2603/tcp	# RIPngd vty
ospfd	2604/tcp	# OSPFd vty
bgpd	2605/tcp	# BGPd vty
ospf6d	2606/tcp	# OSPF6d vty
afbackup	2988/tcp	# Afbackup system
afbackup	2988/udp	# Afbackup system
afmbackup	2989/tcp	# Afmbackup system
afmbackup	2989/udp	# Afmbackup system
xtell	4224/tcp	# xtell server
fax	4557/tcp	# FAX transmission service (old)
hylafax	4559/tcp	# HylaFAX client-server protocol (new)
pcrd	5151/tcp	# PCR-1000 Daemon
noclog	5354/tcp	# noclogd with TCP (nocol)
noclog	5354/udp	# noclogd with UDP (nocol)
hostmon	5355/tcp	# hostmon uses TCP (nocol)
hostmon	5355/udp	# hostmon uses UDP (nocol)
postgres	5432/tcp	# POSTGRES
postgres	5432/udp	# POSTGRES
mrtd	5674/tcp	# MRT Routing Daemon
bgpsim	5675/tcp	# MRT Routing Simulator
canna	5680/tcp	# cannaserver
sane	6566/tcp saned	# SANE network scanner daemon
ircd	6667/tcp	# Internet Relay Chat
ircd	6667/udp	# Internet Relay Chat
ircd-dalnet	7000/tcp	# IRC - Dalnet
ircd-dalnet	7000/udp	# IRC - Dalnet
webcache	8080/tcp	# WWW caching service
webcache	8080/udp	# WWW caching service
tproxy	8081/tcp	# Transparent Proxy
tproxy	8081/udp	# Transparent Proxy
omniorb	8088/tcp	# OmniORB
omniorb	8088/udp	# OmniORB
mandelspawn	9359/udp mandelbrot	# network mandelbrot
amanda	10080/udp	# amanda backup services
kamanda	10081/tcp	# amanda backup services (Kerberos)
kamanda	10081/udp	# amanda backup services (Kerberos)
amandaidx	10082/tcp	# amanda backup services
amidxtape	10083/tcp	# amanda backup services
smsqp	11201/tcp	# Alamin SMS gateway
smsqp	11201/udp	# Alamin SMS gateway
xpilot	15345/tcp	# XPilot Contact Port
xpilot	15345/udp	# XPilot Contact Port
isdnlog	20011/tcp	# isdn logging system
isdnlog	20011/udp	# isdn logging system
vboxd	20012/tcp	# voice box system
vboxd	20012/udp	# voice box system
binkp	24554/tcp	# Binkley
binkp	24554/udp	# Binkley
asp	27374/tcp	# Address Search Protocol
asp	27374/udp	# Address Search Protocol
dircproxy	57000/tcp	# Detachable IRC Proxy
tfido	60177/tcp	# Ifmail
tfido	60177/udp	# Ifmail
fido	60179/tcp	# Ifmail
fido	60179/udp	# Ifmail

Local services

Hasta ahora en Hack x Crack hemos "jugado" con el **Puerto 21** (FTP), el **Puerto 80** (WEB) y poco más. Por petición de algunos y para sorpresa de otros os hemos ahorrado el trabajo de buscar los Servicios que se esconden tras cada puerto. Ya os hemos explicado en anteriores números qué es eso de un Servicio.

EMULE: EL NUEVO REY DE LAS REDES P2P

COMPARTE TUS PROGRAMAS

¿Has perdido un programa que compraste hace poco? ¿Se te ha rallado el CD de tu juego preferido? ¿Has perdido la clave de registro de un programa y no puedes instalarlo? ¿Necesitas un programa y no sabes dónde conseguirlo?

TU SOLUCIÓN ES: eMule

1.- Anteriormente...

En los números anteriores os recomendamos utilizar el eDonkey (www.edonkey2000.com) para solucionar ese problema que todos tenemos de vez en cuando, ya sabes, necesitas instalar un programa pero tu CD ORIGINAL está destrozado y no hay manera de leer los datos. Con el eDonkey te conectabas a una red P2P en la cual encontrabas "copias de seguridad" de TODOS los programas que te puedas imaginar :)

Olvídate YA del eDonkey, el NUEVO REY es eMule. Vamos a ahorrarte unas cuantas horas de trabajo y te diremos qué versión es "la buena" (al menos desde nuestro punto de vista :)

El eMule...

El eMule utiliza la misma red que el eDonkey, es decir, las "copias de seguridad" que puedes bajarte con el eDonkey son las mismas que te podrás bajar con el eMule; pero el eMule es bastante más rápido y tiene mejores opciones (en nuestra opinión, por supuesto)

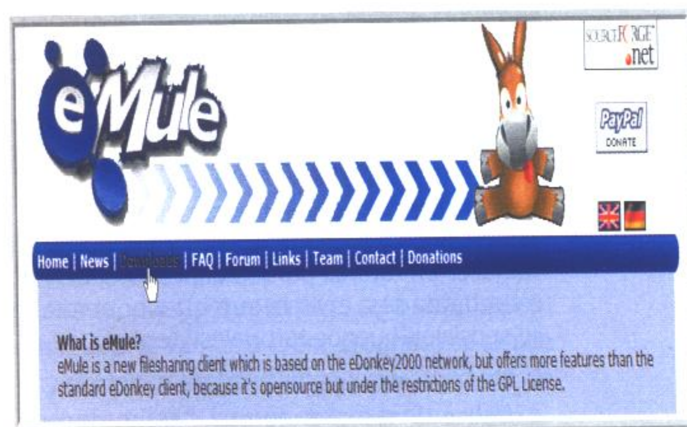
La Red del...

La red del eDonkey (y el eMule) tiene una importante participación de Países de habla hispana, por lo que posiblemente sea la mejor red que existe actualmente para "recuperar" tus copias de seguridad en "spanish" :)

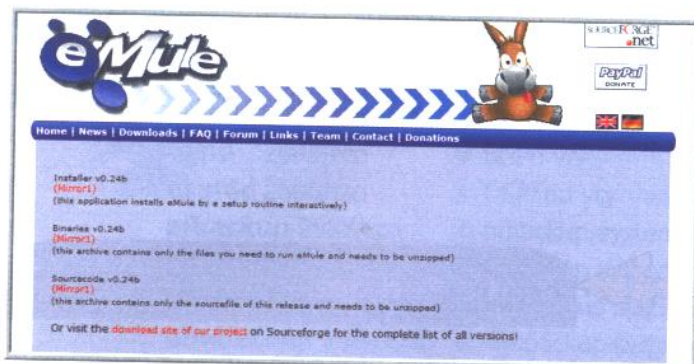
2.- ¿Dónde puedo conseguir el eMule?

El eMule está en continua evolución y tiene muchísimos mods (modificaciones/añadidos), hay peleas entre los "modders" debido a diferencias de opinión respecto a la filosofía de los créditos (contra mas compartes más "credito" tienes para descargar) y si no estás al tanto puedes perderte un poco entre tantas versiones.

En el momento de escribir este artículo la versión disponible en http://www.emule-project.net/ es la 0.24b. Nada más entrar picas sobre la opción downloads



y llegarás a la zona de descargas



Aquí puedes descargarte el programa pulsando sobre el primer "mirror1" o acceder a un centro de versiones (pulsando sobre download site of our project) donde incluso dispones del código fuente de cada una de las versiones :)

emule

0.24b		**2002-12-23 16:00**	
eMule0.24b_installer.exe	899410	893285 i386	exe (32-bit Windows)
emule0.24b-source.zip	962346	73401 i386	Source .zip
emule0.24b.zip	753935	203568 i386	zip
0.24a		**2002-12-16 15:00**	
eMule0.24a_installer.exe	896713	345064 i386	exe (32-bit Windows)
emule0.24a-source.zip	996454	34731 i386	Source .zip
emule0.24a.zip	751485	86374 i386	zip
0.23b		**2002-12-01 16:00**	
eMule0.23b_installer.exe	851287	463384 i386	exe (32-bit Windows)
emule0.23b-source.zip	944142	66626 i386	Source .zip
emule0.23b.zip	718877	108504 i386	zip
0.23a		**2002-11-26 16:00**	
eMule0.23a_installer.exe	841874	119192 i386	exe (32-bit Windows)
emule0.23a.zip	707970	51225 i386	zip
emule0.23a-source.zip	926894	18095 i386	Source .zip
0.22c		**2002-11-13 16:00**	
eMule0.22c_installer.exe	786166	243906 i386	exe (32-bit Windows)
emule0.22c-source.zip	833061	46281 i386	Source .zip
emule0.22c.zip	650507	165083 i386	.zip
0.22b		**2002-11-08 16:00**	
emule022b-source.zip	912834	25788 i386	Source .zip

Disponer del...

Disponer del código fuente significa que puedes leer y modificar el código del programa, ahora que nos meteremos en los cursos de programación sería muy interesante que empezases a "curiosear" en el código de los programas. Por cierto, no se te ocurra pedirle a Microsoft que te de el código fuente de Windows para "curiosear" ¿eh? He, he… Microsoft NUNCA te dará el código fuente de sus programas y mucho menos te dejará modificarlo ;p … pero siempre te queda LINUX, cuyo código fuente está disponible para quien lo quiera :)

Un vez descargado el programa lo instalamos, ejecutamos y a disfrutar. Por cierto, no vamos a hacer un tutorial porque tienes EXCELENTES comunidades en la Red que ponen a tu disposición buenos tutoriales y en cuyos foros te resuelven cualquier duda :)

Cuando instales...

Cuando instales el eMule, verás que te pregunta por el idioma. Pues si, para regodeo de los muchas veces olvidados "hispano-parlantes", podrás seleccionar Español :)

Imprescindible visitar:
* http://www.eshocked2k.com/ --> Una de las mejores comunidades edonkey-maníacas que existe, en perfecto español y con un buen foro.
* http://www.spanishare.com/ --> ¿Buscas algún programa/juego/película? ;p
* http://www.sharereactor.com/ --> En Ingles, si, pero muy "potente" :)

3.- ¿Quieres una copia de seguridad del Visual Studio?

Tan solo tienes que ejecutar el eMule, pulsar sobre el icono BUSQUEDA, seleccionar el cuadro BUSQUEDA GLOBAL, escribir --> visual español <-- dentro del cuadro NOMBRE y pulsar COMENZAR :)



* Si quieres una versión del Visual Studio que incluye lo mínimo (Visual C++, Visual BASIC y poco más) busca un archivo de unos 238 Megas llamado Microsoft. Visual. Studio.6.0.(Visual .Basic.y.C++).[1.solo.CD.+.serial]..., en el número 5 de PC PASO A PASO ya te explicamos la forma de leer (y quemar) este archivo.

* Si quieres la versión completa del Visual Studio deberás bajarte 6 archivos que corresponden a los 6 CDs del Visual Studio: Visual Studio 6.0 español (CD 1).zip, Visual Studio 6.0 español (CD 1).zip, Visual Studio 6.0 español (CD 1).zip, Visual Studio 6.0 español (CD 1).zip, Visual Studio 6.0 español (CD 1).zip y Visual Studio 6.0 español (CD 1).zip

NUEVA SECCIÓN EN PC PASO A PASO: PROGRAMACIÓN DESDE CERO

Ya no tienes excusa para empezar a programar, déjate seducir por el mundo de la programación: prometemos NO ABURRIRTE!!!

1.- Consideraciones Generales:

A petición de nuestros lectores y en la línea habitual de PC PASO A PASO iniciamos este mes una nueva sección: Programación desde Cero. Te introduciremos poco a poco en el "arte" de la programación, pero claro, estás leyendo una revista que no puede limitarse a hacer lo que hace todo el mundo, así que nos hemos propuesto una meta: **QUE NADIE SE SALTE ESTA SECCIÓN!!!**

Si has comprado esta publicación es porque tienes inquietudes (curiosidad) respecto a temas que no suelen tratarse en el resto de revistas informáticas y, por esa razón, DEBES acercarte YA a algún que otro lenguaje de programación. Bueno, eso ya lo sabes, estoy seguro, nosotros podemos seguir explicándote (introduciéndote) en el mundo del hacking PERO si no empiezas a CREAR TUS PROPIOS PROGRAMAS el objetivo de esta publicación no se cumplirá. Preferimos dejar de editar antes que ser una escuela de lamers.

Antes de empezar con esta nueva sección hemos realizado un estudio y hemos descubierto algo realmente ASOMBROSO, el 92% de las personas que compran revistas de informática NUNCA HAN CREADO UN PROGRAMA. Lo más triste es que las revistas de informática más conocidas son aquellas que NO TIENEN cursos de programación, es decir, que la sociedad española parece sufrir una extraña enfermedad: nos gusta la informática pero únicamente leemos panfletos de publicidad tipo PC WORLD o PC ACTUAL. No tenemos nada en contra de estas revistas, es mas, nosotros las compramos cada mes porque informan de los nuevos productos (hard y soft) que salen al mercado y es una buena forma de comparar precios con la tienda de informática de la esquina, esa en la que ya te conocen y atienden bien (dentro de lo que cabe, claro). Por otro lado, parece ser que a todo el mundo le gustaría aprender a programar, pero al "gran público" le parece complicado y de los pocos que compran alguna revista técnica de programación la mayoría acaban dejándolo por imposible porque dicen **NO ENTERARSE DE NADA.**

***** ¿Qué está ocurriendo? *****

No queremos entrar en polémica pero te aseguramos una cosa: si Linux fuese el S.O. (Sistema Operativo) dominante el porcentaje se invertiría, el 90% de simples usuarios tendría, como mínimo, "primerizas" nociones de programación. Esta no es una observación gratuita, te lo aseguro, es UNA REALIDAD. El que se esté preguntando el motivo de esta sentencia es que nunca se ha instalado LINUX, así que, si quieres descubrir el misterio tendrás que instalar, por ejemplo, el **SUSE LINUX 8.1** que sorteamos en la revista ;p

2.- Hemos empezado por Visual Basic.

El director de esta publicación se desespera cuando tiene que publicar un Curso de Programación, no es que no quiera, no, es que la revista tiene por ahora casi 70 páginas y eso es **MUY POCO**. Hay mucho que decir y muy poco espacio... es para echarse a llorar. PERO en los momentos difíciles se agudiza el ingenio, así que vamos a intentar ofreceros **CURSOS EMINENTEMENTE PRÁCTICOS,** intentaremos eludir toda la paja e incluso la teoría (conste que la teoría no es paja).

Quien lea esta sección y ya tenga nociones de programación la encontrará solemnemente aburrida, puesto que el nivel será muy básico. Pero OJO!!! Vamos a crear programitas desde el principio y ya puedes suponer qué tipo de "programitas" vamos a crear ¿verdad?...

je, je... ya verás... seguro que te gustan ;)

Hemos decidido empezar por VISUAL BASIC porque es, con diferencia, el lenguaje más fácil de aprender. Si tuviésemos dinero para publicar una revista de 200 páginas habríamos empezado unos 6 cursos al mismo tiempo, cada uno de un lenguaje diferente, pero por ahora la revista no da para más :(

3.- ¿De dónde me bajo el Visual Basic? ¿Qué es el Visual Basic = Visual Studio?

En el número anterior ya explicamos de dónde bajarlo y cómo instalarlo e incluso te enseñamos a compilar el NETCAT :). De todas maneras, si el "dire" no me ha engañado, en este mismo número te volverán a "orientar" sobre el tema ;) En concreto te dirán donde encontrar el Visual Studio(Visual C y Visual Basic).

Así pues, pasamos a solventar una duda que nos han remitido por mail: nos han preguntado si deben buscar el Visual Studio o el Visual Basic. Vamos a aclararlo de una vez por todas:

* El VISUAL STUDIO es un conjunto de programas entre los cuales se incluye el Visual Basic y el Visual C++.

* El Visual Basic te permite programar en Basic (por decirlo de una forma ridículamente simple).

* El Visual C++ te permite programar en C++.

* Tanto uno como otro pueden comprarse (o descargarse de Internet) por separado O puedes descargarte el Visual Studio y ya tienes los dos en un solo "paquete" :)

* Es Visual Studio es como el Microsoft Office, que incluye WORD, ACCESS, EXCEL, etc. Puedes comprar el Word por separado o el conjunto completo.

4.- ¿Por qué empezamos dos cursos de Visual Basic al mismo tiempo?

Si lees bien los títulos de esta sección verás que solo hay un curso de Visual Basic (el primero: CURSO DE VISUAL BASIC). El objetivo de este curso es el aprendizaje propiamente dicho y durará unos meses :)

El segundo "curso" (IPHXC: EL TERCER TROYANO DE HACK X CRACK (PC PASO A PASO), aunque explicará muchas veces conceptos ya "tocados" durante el primero, tiene un objetivo MUY DISTINTO, crear desde cero un programa muy interesante que hemos llamado IPHXC. Este "curso" durará mucho menos que el anterior y no te desvelamos en este artículo el objetivo de este programa, pero ya irás viéndolo a medida que lo construyamos :)

5.- ¿Algo más?

Solo decirte que empezaremos cursos de C++, APACHE, IIS, PHP, SQL... pero poco a poco, queremos primero que critiques nuestro curso de Visual Basic y aprender de las mismas. Nosotros no hemos hecho nunca cursos de ningún lenguaje de programación y no sabemos si te gustarán o no (esperemos que si :)

Ya está, no te doy más la lata... solo te recuerdo que puedes pasarte por nuestro foro en www.hackxcrack.com y consultar tus dudas con el resto de lectores.



CURSO DE VISUAL BASIC

PARTE I: Bienvenidos al maravilloso mundo de la programación

1. Introducción: Conozcámonos

Antes de empezar, me vais a permitir que me presente. Soy Pedro del Valle, y trabajo como programador profesional. La intención de este curso es iniciar a aquellas personas que sienten la curiosidad de saber como funciona cualquier programa, aplicación o software, ya que todo lo citado es creado por programadores y existen gracias a la programación. Durante los diferentes cursos que se impartirán en la revista hackxcrack vamos a intentar dejar un poco a parte la teoría y ceñirnos a la práctica. Seguramente te estarás preguntando, ¿por qué?, Pues porque la teoría, todo y que es la base de una buena programación, no está incluida en la finalidad real de un curso como el que este pretende ser.

El curso intentará que tu, desde tu PC, puedas desarrollar las mismas aplicaciones que desde aquí vamos a crear, y que cuando obtengas el fruto de tu trabajo, hallas adquirido la habilidad de modificarlas o crear otras que se adapten a tus necesidades sin la ayuda de nadie (exceptuando las MSDN, claro).

Por último comentar que este curso de programación estará orientado a entornos visuales no relacionados con web, aunque si se verán conexiones por puertos, pero cada cosa a su tiempo, y como algunos ya sabrán, lo primero es el "hello world". En cada artículo que leáis tendréis una breve descripción teórica necesaria para entender que es lo que estamos haciendo.

2. La herramienta: Visual Basic

Seguro que mas de uno se estará preguntando ahora mismo el porque de utilizar Visual Basic, si en todos los rincones de Internet dicen que C/C++ es muchísimo mejor. C/C++ es un lenguaje de programación estupendo, muy bueno, te permite rascar el PC a su nivel más bajo, trabajando con interrupciones si hace falta. Pero a su vez es engorroso, muy lineal, anticuado y cada vez con menos salida profesional, y es esta última razón la que me ha hecho decantar por VB 6.0, ya que para aquellos que os queráis dedicar profesionalmente a esto, tarde o temprano os daréis cuenta de que los entornos de Microsoft, Sun y en general los visuales o la programación web son los que actualmente tienen mas salida en el mercado.

Después de esta charla, dejad que os diga una cosa: no dejéis de estudiar C/C++, ya que yo lo considero muy importante como lenguaje base.

Otra razón por la que utilizamos VB es la amigabilidad del entorno de desarrollo. Si hiciésemos una pequeña agenda en C, pocos la acabarían correctamente, mientras que en VB, ya sea por el abanico de opciones en sus menús o por la claridad de los mas que posibles errores producidos durante en tiempo de ejecución, seguro que todos la lograríamos terminar.

3. Lo necesario: Empieza la práctica

Como ya he comentado no voy a entretenerme en la teoría de la programación, solo quiero que sepáis que VB (desde ahora Visual Basic será VB) es un lenguaje de programación orientado a objetos (según unos) o/y a eventos (según otros). Bajo mi punto de vista, VB está orientado tanto a eventos como a objetos, pero realmente no nos importa, aquí cada uno dará la versatilidad necesaria al compilador. Lo primero que necesitáis es el VB 6.0, que podréis encontrar en el paquete Visual Studio 6.0

Es mi deber indicar que VB no es freeware, sino que es un producto de Microsoft el cual tiene una licencia que tienes que pagar antes

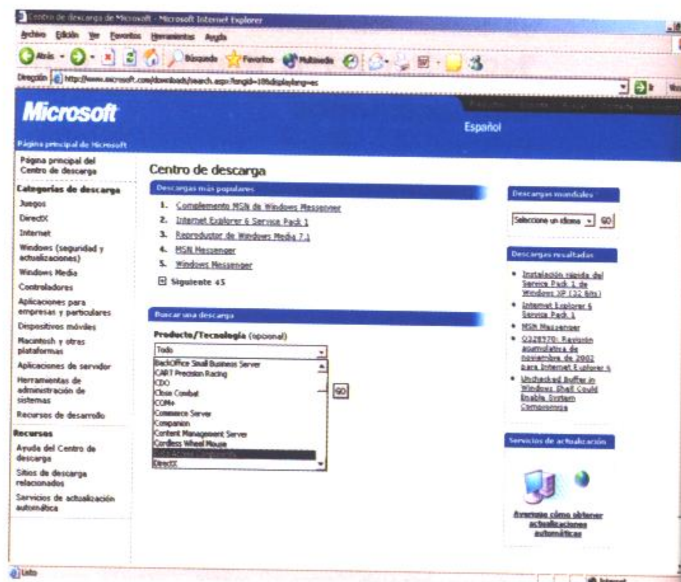
de poder utilizarlo, ya sea en enseñanza o desarrollo.

La instalación es bastante sencilla, si solo tenéis el CD de VB, estamos ante un clásico de las instalaciones: "Siguiente, siguiente, acepto el contrato, siguiente... ".

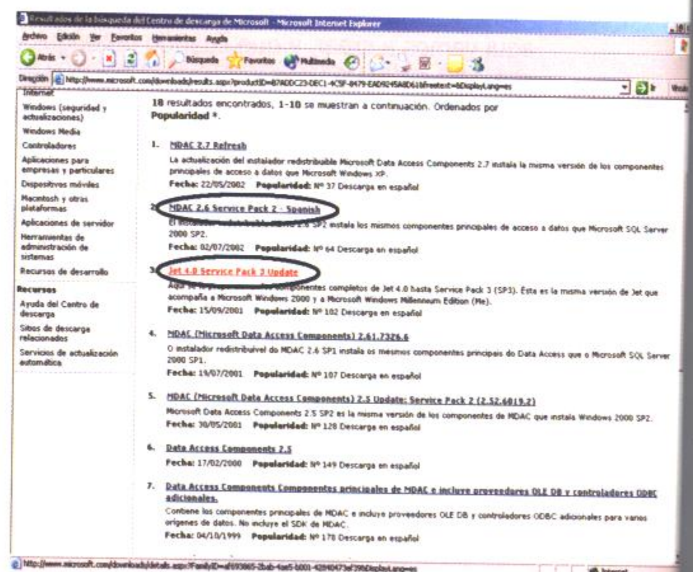
Si por el contrario tenemos los CD del Visual Studio, podemos hacer dos cosas, elegir instalación personalizada y seleccionar solo el "check" de VB, o instalar todas las herramientas que están en el CD (recomendado). ¿Ya está instalado?, bien, pues ahora podríamos instalar el SP (Service Pack) del VB, que encontrarás en la página de http://www.microsoft.com. Si no lo instalas, podrás trabajar igualmente, pero es recomendable. Lo que si es imprescindible es que actualices los gestores de BBDD para futuras aplicaciones, para ello debes ir a la página de Microsoft y bajar los instalables Microsoft Jet SP3 y MDAC 2.6 o 2.7 Para encontrar estos productos debemos ir a http://www.microsoft.es, hacemos clic en "área de descarga"



Nos aparecerán dos combos de selección. Desplegamos el primero y escogemos "Data Access Components"



Hacemos click en el botón "go". Nos aparecerá una página con varios componentes para instalar, nosotros necesitamos exactamente el "Jet 4.0 Service Pack 3 Update" y el MDAC 2.6 Service Pack 2 - Spanish.



Una vez bajados, los instalamos, ya estamos listos para empezar.

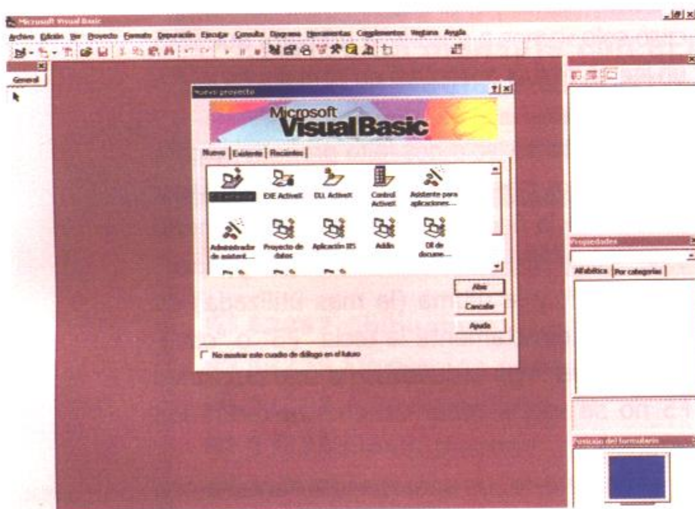
Bien, hoy vamos a hacer el famoso hello world. ¿Y en que cosiste?, el hello world Es un mito entre los programadores, se trata de que, cuando se empieza a estudiar un nuevo lenguaje de programación, y se empieza con la practica, crear un programa que con su ejecución muestre

Una vez bajados, los instalamos, ya estamos listos para empezar.

Bien, hoy vamos a hacer el famoso hello world. ¿Y en que cosiste?, el hello world Es un mito entre los programadores, se trata de que, cuando se empieza a estudiar un nuevo lenguaje de programación, y se empieza con la practica, crear un programa que con su ejecución muestre un mensaje por pantalla que muestre el literal hello world o en su defecto, "hola mundo".

Para llevar a cabo esto, tenemos que abrir el visual basic, lo encontraremos en Inicio -> Programas -> Microsoft Visual Studio -> Microsoft Visual Basic 6.0 en el caso de los que instalasteis el Visual Studio, y para los que solo instalasteis el Visual Basic lo encontrareis en Inicio -> Programas -> Microsoft Visual Basic 6.0

Al iniciar la aplicación nos aparecerá una ventana madre con otra hija que no nos permitirá continuar hasta que elijamos una opción.



Bien, para nuestra prueba de hoy, no explicaré las diferentes opciones de esta ventana, ya que eso será en futuras entregas. Solo deciros que aquí elegiremos el tipo de proyecto que vamos a crear, es decir, un ejecutable, una DLL, un OCX...

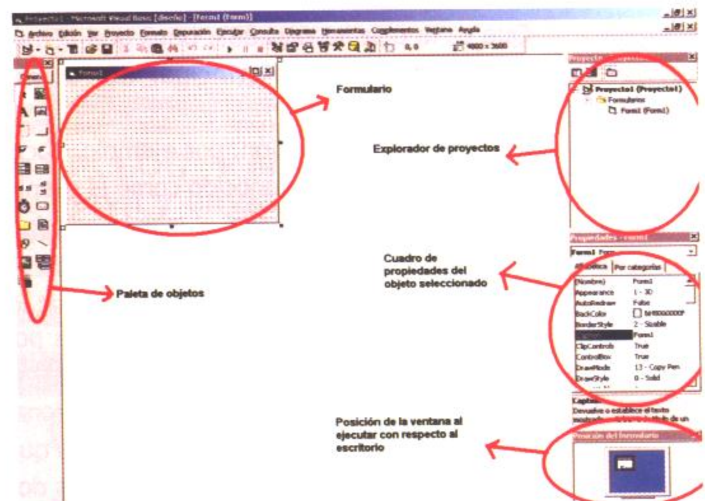
Nosotros, para nuestra primera aplicación vamos a elegir "EXE estándar", ya que nuestro

Bien, para nuestra prueba de hoy, no explicaré las diferentes opciones de esta ventana, ya que eso será en futuras entregas. Solo deciros que aquí elegiremos el tipo de proyecto que vamos a crear, es decir, un ejecutable, una DLL, un OCX...

Nosotros, para nuestra primera aplicación vamos a elegir "EXE estándar", ya que nuestro programita será un ejecutable.

Cuando le demos a aceptar, nos aparecerá nuestro entorno de trabajo, que en un principio solo constará de un formulario, llamado por defecto "Form1".

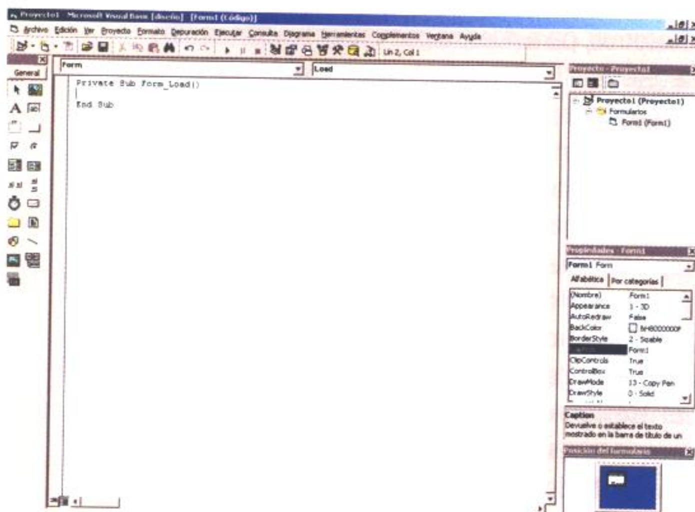
También nos deberían aparecer varias paletas, a la izquierda tenemos los objetos por defecto que podemos añadir al formulario, a la derecha, el explorador de proyectos, el cuadro de propiedades del objeto seleccionado y la posición inicial del formulario en pantalla.



Bien, en esta sesión no explicaremos nada sobre los diferentes objetos o sobre el cuadro de propiedades, ni tan solo explicaremos los menús del Visual Basic, sino que iremos directos al grano y crearemos un programa que al ejecutarse imprima el mensaje hello world por pantalla (recordad que siempre debéis curiosear vosotros mismos).

En futuros artículos explicaremos todo lo que hoy nos dejamos pendientes, no os preocupéis por eso.

Vale, supongo que estáis listos, haced doble click sobre el formulario. Inmediatamente os tendría que aparecer un editor de texto con dos líneas de código escritas, y el cursor entre ellas.



Qué es lo que ha pasado?, pues que hemos accedido al evento principal del objeto formulario.

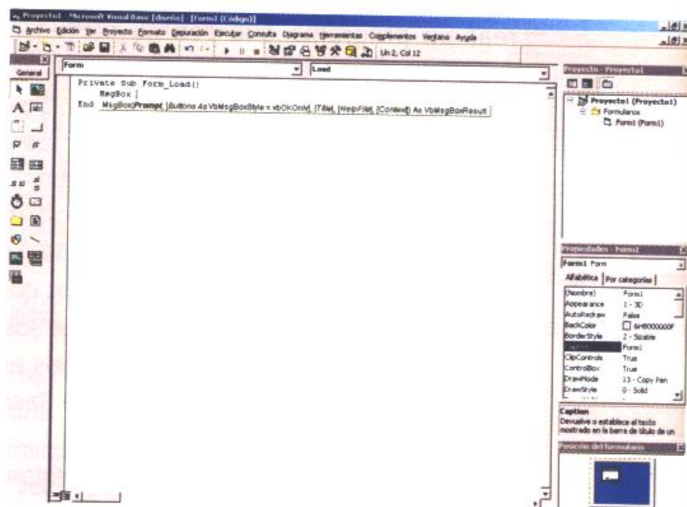
Un evento es una acción, por ejemplo, hacer click en un botón es conocido como el evento button_click. En este caso, el evento principal de un formulario es el form_load. ¿Y que es el form_load?, muy fácil, es el evento que se activa cuando ejecutamos el programa por primera vez, es decir, que cuando se inicie la aplicación que estamos creando se va a accionar el form_load. ¿Que conlleva esto?, pues que todo el código que escribamos entre las dos líneas que nos han aparecido anteriormente se va a ejecutar al iniciar el programa (al ejecutarse el form_load), y así con todos los eventos.

Una vez entendida esta teoría, vamos a ponerlo en práctica. Para mostrar un mensaje por pantalla (la clásica ventana con el botón aceptar) utilizaremos un objeto que viene por defecto en Windows llamado MsgBox.

Escribiremos entre las dos líneas, es decir, dentro del evento load (fijaos que pone Form_Load()) la siguiente línea:

MsgBox "Hello world"

Muy probablemente, al escribir MsgBox y pulsar la barra espaciadora os ha aparecido una línea amarilla con información. Esta información es una ayuda para el programador, y nos está indicando que parámetros podemos pasarle al MsgBox



Los parámetros son diferentes opciones que podemos pasar a los objetos del VB. En este caso solo vamos a pasarle el primero, que será un literal, el cual aparecerá en pantalla en forma de mensaje.

Una vez escrito, solo nos falta probarlo, y para ello tenemos tres opciones, la primera es hacer click sobre la flecha azul que hay en el menú superior, la segunda es ir al menú "Ejecutar" e "Iniciar", y la última (la mas utilizada) es presionar directamente la tecla "F5" o "ctr + F5" para ser mas cautelosos (si solo pulsamos F5 no se van a tener en cuanta todos los errores).

Si al hacer esto, os aparece una ventana con un botón aceptar y el mensaje Hello world"

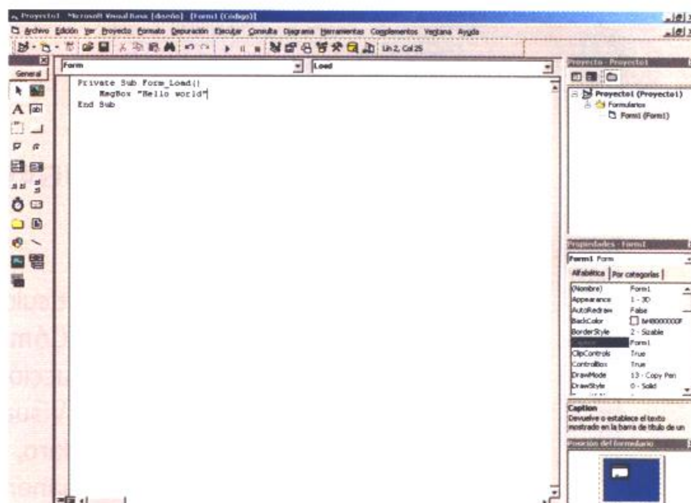


Lo habéis hecho bien, si os da cualquier error, fijaos en la IMAGEN, ya que ese es el código de vuestro programa. Después de pulsar aceptar, veréis que os aparece un formulario en blanco, no os preocupéis, es el form inicial de nuestro proyecto, el cual no tienen ningún objeto porque no se lo hemos puesto.

Aquí os dejo, y aunque tenéis poco para practicar, os recomiendo que probéis cosas, como intentar enviarle mas parámetros al MsgBox.

Un saludo, y suerte.

El mes que viene seguiremos con la segunda parte de este curso.



IPHXC: EL TERCER TROYANO DE HACK X CRACK (PC PASO A

PARTE I: EMPEZANDO A JUGAR CON VISUAL BASIC

Cuándo se planteo el realizar este articulo, me surgieron varias dudas, ¿Cómo redactar adecuadamente una introducción a un programa tan extenso como Visual Basic?. El espíritu de la revista es claro, -"Enfocar las explicaciones de una manera sencilla, clara y pensando sobre todo en los lectores que se inician en este nuevo campo"- Vale, hasta ahí bien, el problema es no caer entonces en explicaciones excesivamente técnicas, pero.... tampoco caer en aberraciones informáticas demasiado escandalosas, a riegos de que algunos de los lectores pidan mi cabeza en bandeja de plata, intentare un equilibrio entre estos dos conceptos, para que quien no este familiarizado con VB, lo entienda lo mejor posible y quien ya este ducho en estos temas, le sirva solo como recordatorio de aquellos créditos que no sabían donde utilizar en la universidad.

Bueno, empecemos a entrar en materia, ¿Porque visual Basic?, Soy de la opinión, por supuesto, no necesariamente compartida, de que es un perfecto inicio para quien no tenga practica en lenguajes de programación, es sencillo, potente y muy intuitivo, ¿Mejor que otros?, La eterna pregunta, pues depende para quien y para que. Lo mejor es utilizar el que mejor conozcas y cumpla con tus necesidades.

Por supuesto, lenguajes como C, Delphi, Python, etc, entiendo que requieren al menos unos conocimientos, que no cumplen un elevado tanto por ciento de los lectores de esta revista, ...de momento. Aunque a la larga, es obvio que tarde o temprano se han de tocar en la revista.

Resumiendo, queremos que al terminar este articulo, el lector nuevo, corra a encontrar este programa por que hemos conseguido despertar su interés y su curiosidad por la programación, el crear tu primer programa, con la utilidad que necesitas, es una satisfacción personal muy gratificante, y no lo dudes, "el mejor programa", es aquel que tu has creado.

¿Cómo conseguir Visual Basic?, La revista ya explica en los números anteriores (revista 5) este tema, yo "recomiendo", o bien hacerse con una licencia de estudiante, o su correspondiente "copia de seguridad" en los lugares adecuados.

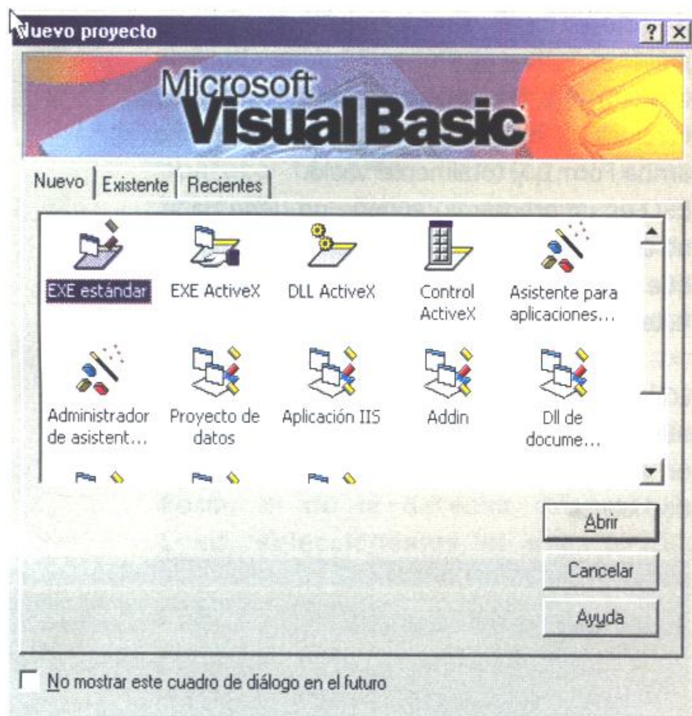
Existen varias versiones de Visual Basic 6, en este articulo usaremos la edición empresarial de Microsoft Visual Studio 6 (Básicamente todas las versiones son parecidas en lo referente a Visual Basic), contiene no solo Visual Basic, si no también C++.

INSTALACION: La revista en su numero cinco ya explico la instalación de Microsoft Visual Studio 6 Edición profesional, con lo cual, lo único, remitiros a su lectura.

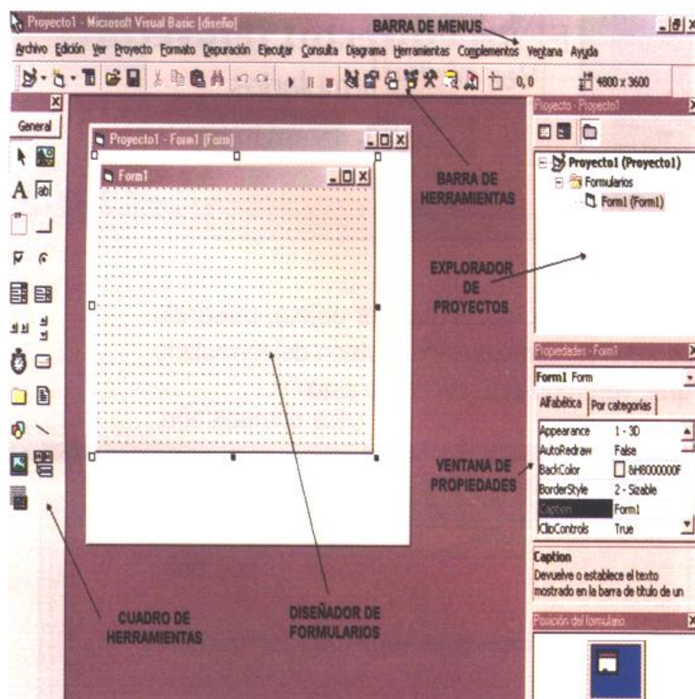
PRIMERA TOMA DE CONTACTO:
Bueno, ya esta instalado, llego el momento esperado.

INICIO-Programas-Microsoft Visual Studio 6.0-Microsoft Visual Basic

El programa arrancara y nos mostrara una pantalla como esta,

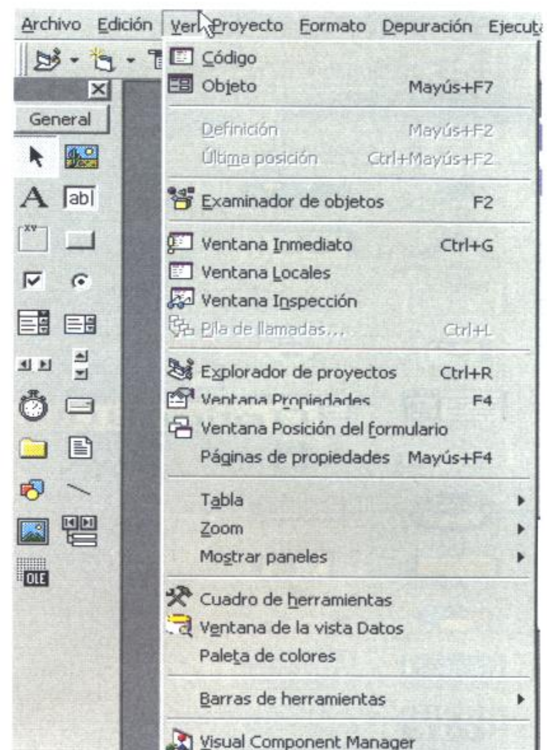


elegiremos Nuevo-EXE estándar-Abrir. Llegados a este punto veremos una pantalla como esta



veamos para que sirve cada cosa:

ATENCION: Si no saliera, podéis activar-desactivar estas opciones en el menú Ver.



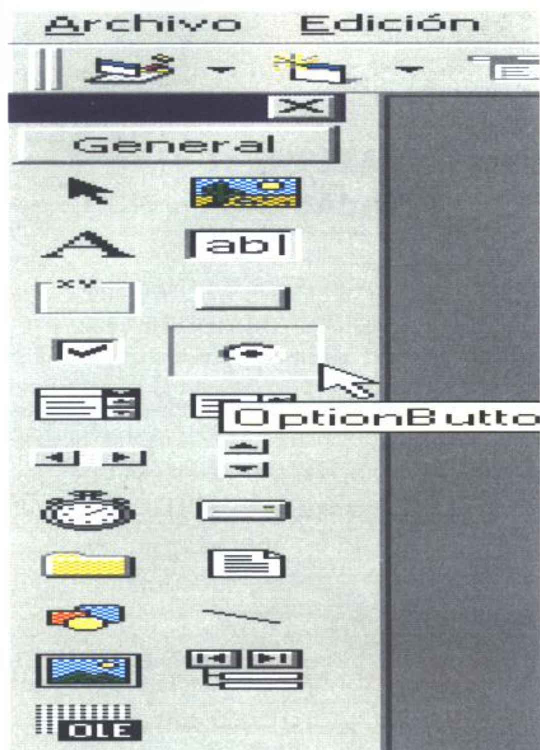
Barra de menús: Las típicas en aplicaciones Windows, mas las especificas de VB.

Barra de herramientas: Para el acceso rápido a los comandos mas usados.

Explorador de proyectos: Enumera los formularios y módulos del proyecto actual. ¿Que es un proyecto?, Pues es un conjunto de archivos, entendiendo por archivos a los formularios y módulos. Formularios y módulos son contenedores del código que creamos. Mas adelante, veremos estos conceptos de forma mas practica.

Ventana propiedades: Enumera los valores de las propiedades del control o formulario seleccionado. ¿Que es una propiedad?, pues es una característica de un objeto, por ejemplo, color, tamaño, etc.....

Cuadro de herramientas: Es un conjunto de herramientas, que podemos usar durante el diseño, para insertar controles en el formulario. ¿Que es un control? Pongamos un ejemplo, fijaros en esta figura, ¿Reconocéis la imagen? Efectivamente, en muchos programas nos encontramos con estas casillas, sirven para seleccionar opciones.



Diseñador de formularios: La parte central y principal, sobre la que más trabajaremos introduciendo código y los controles del cuadro de herramientas. Esta es la interfaz del programa que creemos.

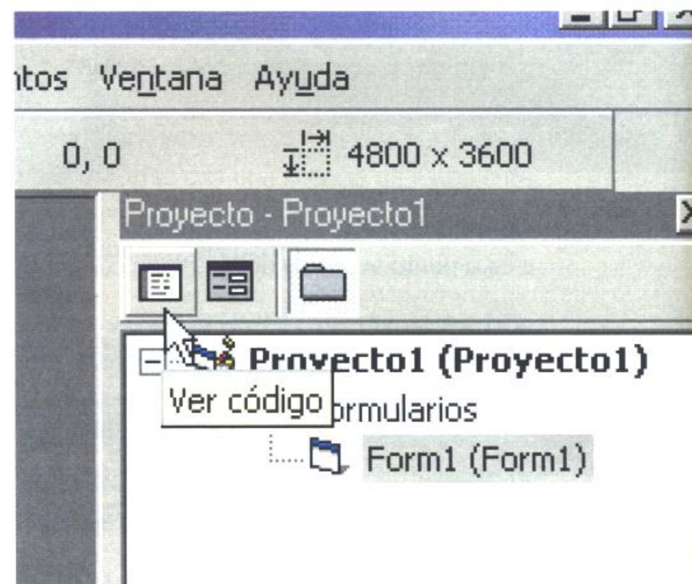
Bien, ya sabemos algunas cosas, ejecutemos nuestra primera aplicación, -¿Ya?-, pues si, veamos como, fijaros en la barra de herramientas, veréis los típicos iconos de Iniciar-Interrumpir-Terminar



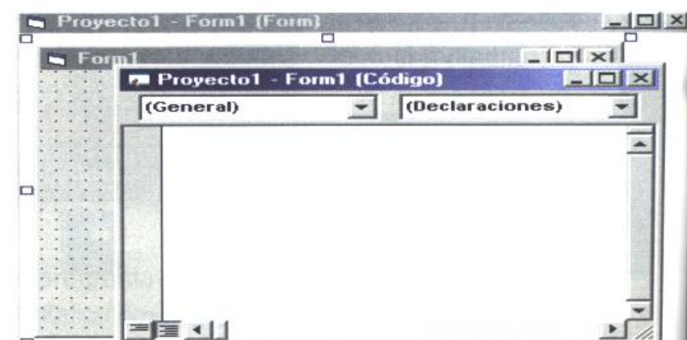
>, solo el icono de iniciar esta habilitado, pulsemos sobre el (Pulsar F5 tiene el mismo efecto), nuestra aplicación se ejecuta, solo veremos un formulario, de color gris, que pone arriba Form1, y totalmente vació.

ESO es un programa, aunque no tiene nada, no ejecuta nada,....... nos queda meter el código que queramos y los controles que nos hagan falta.

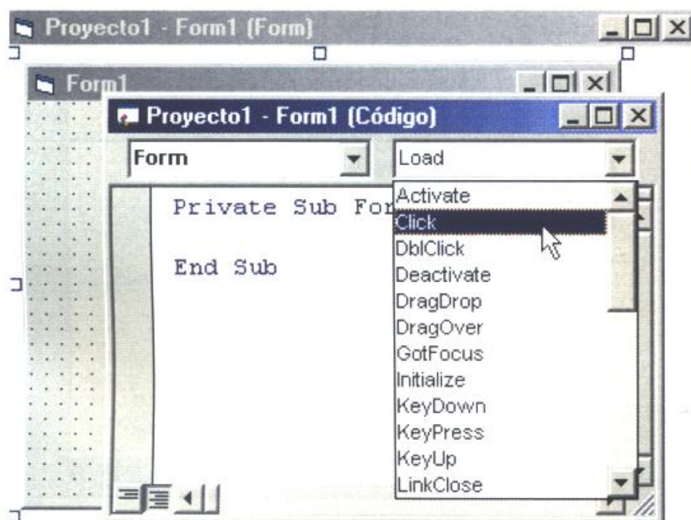
¿Cómo metemos código?, Primero paremos nuestra aplicación pulsando en Terminar, fijaros en el Explorador de Proyectos, arriba veréis dos iconos



uno es Ver código, el otro Ver objeto, pulsando sobre ellos, cambiaremos la visión del formulario gris, veremos algo así como esto



cambio el titulo y pone Form1(Código), debajo vemos dos menús despegables, en concreto pone en el de la izquierda "General", y si pulsamos la flecha nos aparece también, Form(es el único "control" que tenemos de momento. El de la derecha modificara su contenido de acuerdo a la selección anterior, en él nos saldrán los "eventos" de ese control. -¿Eventos? Ya empezamos con palabras raras-, Lo mejor para explicarlos es ver un ejemplo, seleccionemos en el menú despegable de la izquierda Form, el de la derecha cambiara a Load, seleccionemos el evento Clik



nos aparece esto

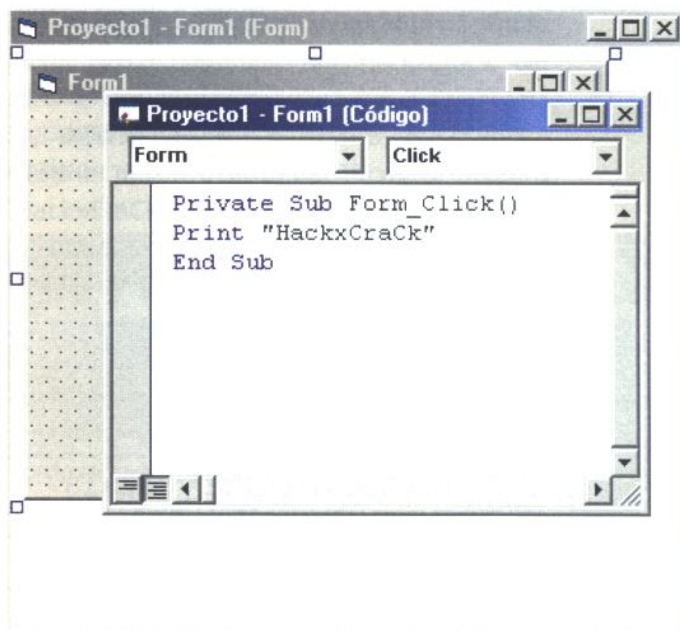
Private Sub Form_Click()

End Sub

Escribamos esta línea en medio

Print "HackxCraCk"

Al final nos quedaría tal como la imagen



Ahora pulsemos F5, arranca nuestra aplicación, ¿no pasa nada?, Espera, ahora "cliclea" sobre el formulario, aparece lo que hemos escrito, HackxCraCk.

¿Que a pasado y porque?, Demos una pequeña explicación, el código de una aplicación de VB se divide en bloques menores llamados procedimientos. Un procedimiento contiene el código que se ejecutara cuando se produce un evento seleccionado.
En este ejemplo el procedimiento o evento es:

Private Sub Form_Click()

End Sub

Private Sub Form= Comienza el procedimiento

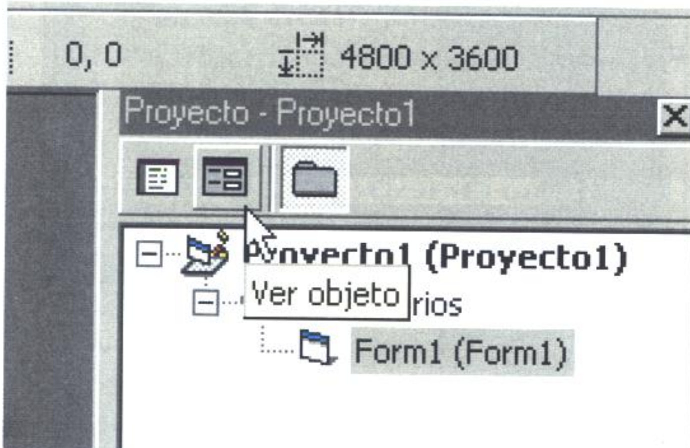
End Sub= Termina el procedimiento

¿De que evento? Click() , evento de hacer clic sobre el formulario

Resumiendo, cuando efectuemos un clic sobre el formulario, se ejecutara el contenido, en este caso:
Print "HackxCraCk"= Imprimir en pantalla lo

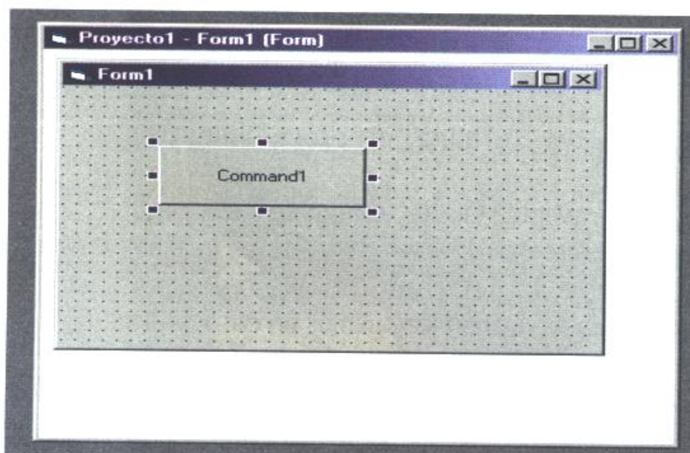
que tengamos encerrado entre comillas.

Pongamos otro ejemplo sencillo, paremos la aplicación, volvamos a pulsar el icono del explorador de proyectos -Ver objeto-



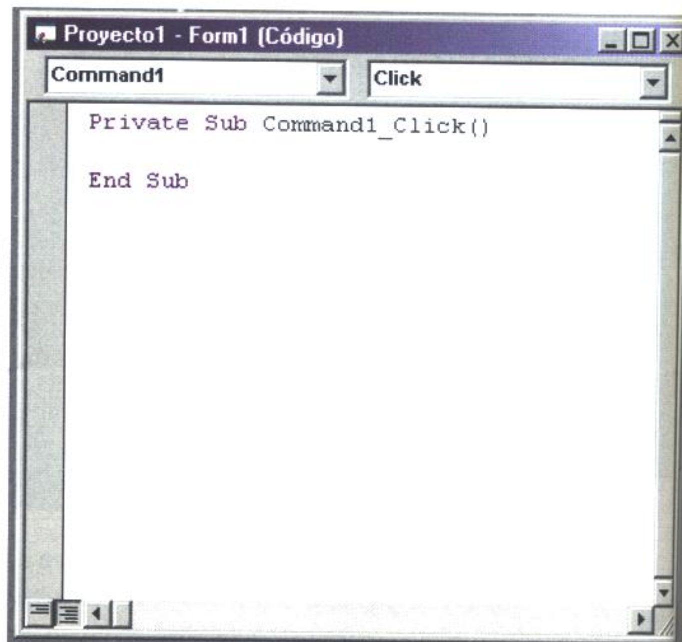


ahora pulsemos en el cuadro de herramientas sobre el icono que representa el Botón de comando, , sobre el Form1 y manteniendo pulsado el botón izquierdo del ratón, creemos un rectángulo,¿ ....ya?, Vale, soltemos el botón del ratón, ya tenemos creado el típico botón de aceptar, anular, enviar, etc....., solo que este pone dentro Command1,...vamos a poner algo mas real, por ejemplo, Imprimir, lo primero seleccionemos ese control, el botón quedara rodeado de unos puntos, como veis en la imagen



Veamos la ventana de propiedades, en ella veremos una lista de propiedades y en azul una que pone caption, a su derecha veremos que pone Command1, bien, ese es el titulo que tiene el botón dentro, cambiémoslo, bien con el ratón o con la tecla TAB, nos pondremos sobre ese apartado, escribimos en este caso Imprimir, o lo que tu quieras, veras como va cambiado el titulo del botón.

Ya esta, ahora cuando nosotros pulsemos el botón, tendrá que hacer "algo",en este caso, pondremos lo mismo que en el ejemplo anterior, HackxCraCk , para lo cual haremos lo siguiente, "clicleemos" dos veces encima del botón, se nos abrirá una ventana como esta.



¿Que evento nos ha salido?, El que nosotros hemos provocado "clicleando" encima del control, el evento Clic del procedimiento Command1.

Escribamos dentro de este procedimiento

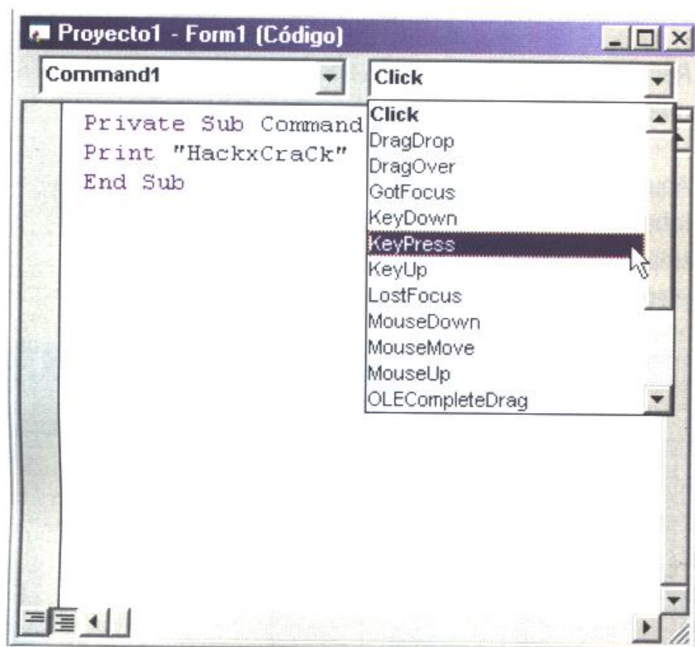
Print "HackxCraks", nos quedara así:

```
Private Sub Command1_Click()
Print "HackxCraCk"
```

End Sub

Vamos a probar, pulsemos F5, y ahora pulsemos sobre el botón, nos saldrá el texto que pusimos entre comillas, tantas veces como "clicleemos" botón Imprimir.

Seamos curiosos, ahora paremos nuestra aplicación, vemos que el control Command1 tiene muchos eventos, despleguemos la lista de la derecha,



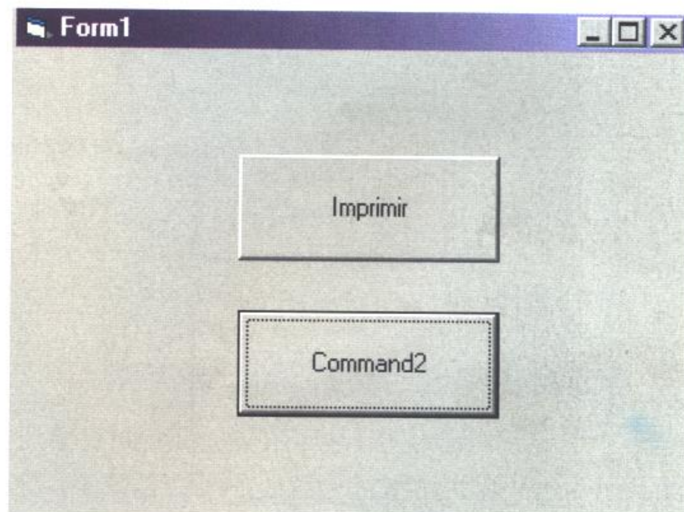
Y seleccionemos otro evento, en este caso vamos a seleccionar KeyPress, borramos o cortamos lo que pusimos en el evento ClicK, y escribimos o pegamos lo mismo en el evento KeyPress, nos quedara algo así

```
Private Sub Command1_Click()

End Sub

Private Sub Command1_KeyPress(KeyAscii As
Integer)
Print "HackxCraCk"
End Sub
```

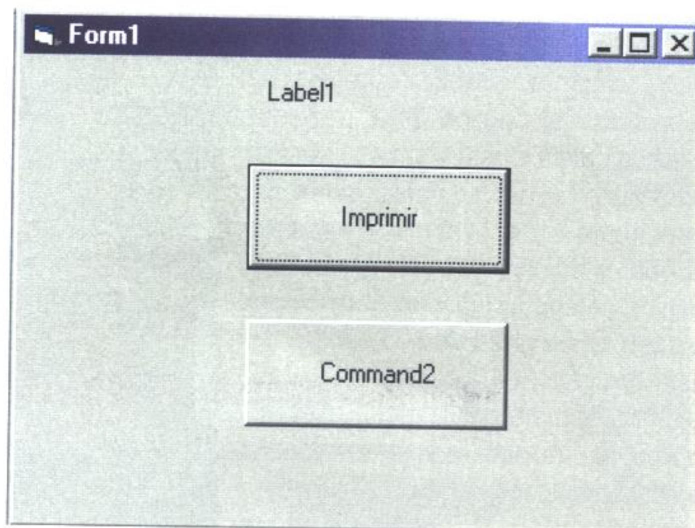
Bien, ahora pulsemos F5, nuestra aplicación arrancara, si pulsamos sobre el botón no pasara nada, lógico, borramos Print "HackxCraCk" del evento Clik, en cambio, pulsar cualquier tecla del ordenador, ...efectivamente, se empieza a rellenar nuestro formulario con la palabra HackxCraCk.¿Porque?, la respuesta es que pusimos Print "HackxCraCk" en el evento KeyPress del control Command1, -Entonces KeyPress es el evento de pulsar cualquier tecla?- , Si, pero solo funciona si el control tiene el foco, -¿El que?- Veamos un ejemplo, paremos nuestra aplicación, volvamos a poner el formulario en modo ver objeto, ahora repitamos la operación de poner otro Botón de Comando, en este caso veremos que se llama Command2, arranquemos nuestra aplicación, pulsemos ahora sobre el botón Command2, queda rodeado por una línea discontinua



ese control es el que tiene el foco, es el control "activo" dentro del formulario, ahora aunque pulsemos cualquier tecla no escribirá nuestra frase en el formulario , pulsemos ahora el botón Imprimir, se pone con ese recuadro de líneas discontinuas, ahora el tiene el foco de la aplicación , si pulsamos cualquier tecla, como en el evento keyPress del control command1(Imprimir) tiene la línea Print "HackxCraCk" , veremos de nuevo en el formulario la consabida frase "HackxCraCk". Resumiendo los eventos de los controles se producen si tienen el foco de la aplicación.



Bueno, paremos nuestra aplicación, veamos otro control, en este caso en el cuadro de herramientas, seleccionemos el control Label, con el formulario de nuestro proyecto en modo ver objeto, creamos otro rectángulo en cualquier parte del formulario(ya sabemos botón izquierdo pulsado), se nos creo un espacio que pone label1, este control es un simple recuadro de texto, si pulamos F5, nuestra aplicación arrancara y nos mostrara esto.



Paremos nuestra aplicación y pongámonos en modo ver código, borremos la línea que pusimos en:

Private Sub Command1_KeyPress(KeyAscii As Integer)
End Sub

Que era :
Print "HackxCraCk"

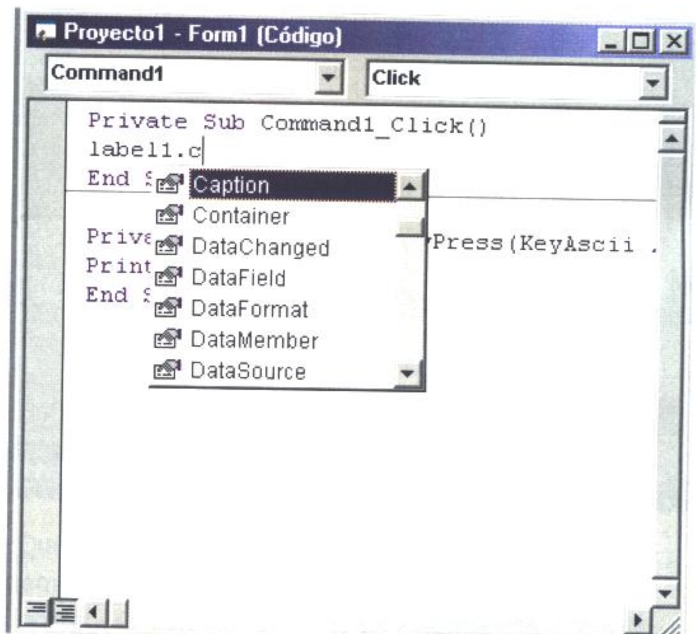
Seleccionemos el control Command1 en el menú despegable, y ahora el evento Clik Vamos a poner "algo" para que la acción de pulsar el botón realice alguna acción sobre el nuevo control Label que hemos creado.

Pongamos lo siguiente:
Label1.caption="HackxCraCk"
Nos quedara algo así:

```
Private Sub Command1_Click()
Label1.Caption = "HackxCraCk"
End Sub
```

Recordar que la propiedad Label es el "texto" que nos sale en el control.

Aquí hemos hecho algo diferente, hemos escrito label1, ponemos un punto(.) y se despliega una lista de propiedades de la que hemos elegido , la propiedad Caption .



Resumiendo, hemos puesto en código, que cuando pulsemos(Clik) en el botón Command1, el objeto label1 cambie su propiedad Caption a la cadena de texto que hemos puesto entre comillas (HackxCraCk).

Probemos si funciona, F5 y pulsar el botón

Imprimir (Command1), aparece la frase dentro del contenedor que es el control Label1.

Paremos nuestra aplicación, seguimos teniendo el botón command2, escribamos dentro de su evento Clik, la siguiente línea
Label1.Caption = "Mi revista!!!!"

Nos quedara algo así como:

```
Private Sub Command1_Click()
Label1.Caption = "HackxCraCk"
End Sub

Private Sub Command2_Click()
Label1.Caption = "Mi revista!!!!"
End Sub
```

Pulsemos ahora F5, y de forma alternativa, "cliclemos" sobre los botones, lo que estáis viendo, no es mas que publicidad encubierta (hay que barrer "pa casa" ;-))

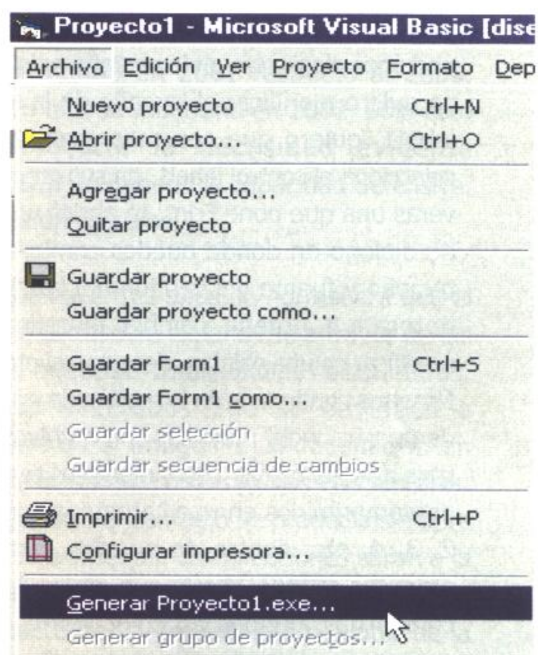
Bueno, nos gusta lo que hemos realizado hasta ahora, llego el momento de guardarlo, paremos nuestra aplicación, nos vamos a la Barra de menú y pulsamos Archivo-guardar proyecto como, y nos sale el clásico dialogo guardar archivo como, lo mejor llegado a este punto es que creéis una carpeta nueva por ejemplo en c:\ y la llameéis PVB(practicas visual Basic), crear una subdirectorio dentro por ejemplo 1, una vez tengamos el directorio, guardemos el archivo Form1.frm (sale por defecto), después saldrá el archivo Proyecto1.vbp, también lo guardamos.

Estos dos archivos son:
Form1.frm= Archivo de formulario, este archivo lo podéis editar con el NotePad, su contenido son los controles que tenemos insertado en el formulario y sus propiedades
Proyecto1.vbp= Archivo de proyecto, también se puede editar con el NotePad, en el veremos las características y referencias de nuestro proyecto.

-Esto esta bien, pero yo quiero enviar a mi prima la de Toledo, un archivo para que vea lo que se hacer, pero le envié estos dos archivos y me dice que no los puede abrir-

Bien, los podrá abrir y ver tu trabajo si dispone del programa VB, de no ser así, lo que tienes que enviarle es el archivo "compilado", un loquesea.exe.

En la Barra de Menús pulsamos Archivo-Generar Proyecto1.exe



Nos saldrá el Cuadro de dialogo Generar proyecto, y por defecto el nombre proyecto1.exe, lo guardaremos en nuestra carpeta c:\PVB\1\.

Bien, ahora tenemos en la ruta c:\PVB\1 el archivo proyecto1.exe, si ejecutamos ese archivo, nuestra aplicación se ejecutara como un programa mas de Windows.

-Vale, todo esto esta muy bien, pero esto es una revista de hack, ¿Cómo relaciono esto con "lo que yo quiero?", Bien, acudamos al refranero, "vísteme despacio, que tengo prisa", en cristiano, "que la paciencia sea nuestra mejor arma".

Es de suponer, que después de esta pequeña introducción, los que nunca utilizasteis VB, al menos no le tengáis miedo (que si respeto). En unas pocas paginas, no podemos explicar como hacer un programa que envié la ip, el archivo pwl o como se llama la maquina donde se ejecuta. Recordar el titulo, Introducción a Visual Basic

-¿Que más cosas se pueden hacer?, Pues por ejemplo si queremos cambiar el color de fondo del formulario(el gris es algo triste), seleccionamos el formulario en modo ver objeto, la propiedad Backcolor es el color de fondo, podemos elegir otro en la pestaña paleta,-Vale, yo quiero modificar el tamaño de la letra del label1, quiero que sea mas grande-, pues selecciona el control label1, en sus propiedades veras una que pone Font, te abrirá un cuadro de dialogo en donde puedes cambiar estilo, tamaño y fuente del caption del label. Ahora te toca a ti, prueba, cambia, investiga, crea, modifica, en una palabra, descubre el programa. Nosotros pondremos en la sección de programas de nuestra web, practicas con archivos de VB para que los bajéis. Estos ejemplos tenéis que descomprimirlos en una carpeta, por ejemplo 2, 3, 4, etc, dentro de nuestra carpeta de practicas c:\PVB. Veréis que en las líneas de código hay algunas en color verde, con un apostrofe delante ('), estas líneas son comentarios, explicaciones del programa, nos comentarios, explicaciones del programa, nos serán de gran ayuda.

Bueno, no se si el objetivo de este articulo se habrá logrado, os toca a vosotros evaluarlo, espero que tenga continuidad, después de la introducción como en todo, viene la "expansión", pero eso depende de la revista y del interés de los lectores por este tema,....el foro tiene la palabra.

PRACTICA 1: Programa oculto a Ctrl+Alt+Supr. En esta práctica podemos ver como ocultar los procesos en win95/98/ME

PRACTICA 2: Programa que nos permite saber nuestra IP.
Todos habéis visto y bajado el programa que se encuentra en nuestra web, y que se llama IP_Agent.exe, este es mas o menos lo mismo, pero hecho por vosotros, (utilizando el control OCX).

PRACTICA 3: Programa que nos permite escribir en el archivo regedit, el programa que tenéis en el foro, careg.exe

EL SIGUIENTE ARTICULO VERSARA SOBRE CONTROLES MÁS COMUNES, SUS EVENTOS Y PROPIEDADES, DEFINICION DE APIS, Y CREACION DEL PROGRAMA IPHXC PASO A PASO.

EL GANADOR DEL SORTEO DE UN SUSE LINUX 8.1
DEL MES DE DICIEMBRE ES:
ISIDRO DOMINGUEZ MARIÑO
VIGO PONTEVEDRA

SEGUIR LLAMANDO, EL PROXIMO PODRIA SER PARA TI (PAG 63)

TENDENCIAS ACTUALES EN CODIGO MALICIOSO: Pronosticos para el año 2003

ELABORADO POR DEPARTAMENTO DE MEDICIÓN DE RESULTADOS DE TRENDLABS - TREND MICRO, INC.

1.- Como es habitual al final de cada año, en las empresas se debate la planificación del siguiente, siendo uno de los temas principales a qué merece la pena destinar el presupuesto disponible.

De varios estudios que sobre el gasto empresarial se han realizado recientemente se desprende que, por lo menos, ahora figuran en los presupuestos partidas destinadas a la protección de las redes internas, que comprenden antivirus, cortafuegos y adquisición de otros productos de seguridad. La cuestión que continúa pendiente es dar con un método con el que los administradores de sistemas puedan predecir la solidez de sus defensas informáticas y transmitan su punto de vista a la alta dirección.

En varias ocasiones se han publicado predicciones relativas a la próxima "bomba" que el código malicioso nos depara para el futuro próximo. Hay que tener en cuenta que la información que se baraja suele pecar de subjetiva por ser incompleta y referida tan sólo a unos meses.

Los datos estadísticos referidos a la cantidad de infecciones sufridas en un determinado periodo de tiempo señalarán únicamente hacia dónde se ha extendido efectivamente los virus que han aparecido, pero no qué tendencias se están imponiendo entre quienes los escriben. Para realizar un pronóstico acertado habría que partir además de los brotes víricos reales surgidos en todo el mundo y documentados por los distintas desarrolladores de antivirus, analizando en cada caso cómo se extendió la infección.

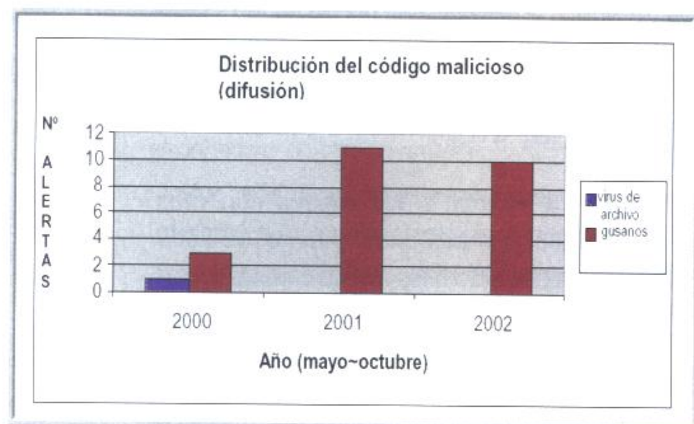
Echando un vistazo a los meses con más movimiento en los tres años que van de 2000 a 2002, y en concreto a los meses comprendidos entre mayo y octubre, se observa un gigantesco aumento, del 175%, de los ataques víricos en todo el mundo en 2001 respecto al 2000, volumen que se mantiene en 2002. Sólo esto ya demuestra la necesidad evidente de mejorar en general la capacidad defensiva. La cuestión es cómo.

2.- Hasta hace tres años, lo normal era que el código malicioso se expandiese a través de las vías de infección tradicionales: disqueteras, ficheros infectados que se enviaban a compañeros y amigos o almacenados en carpetas de acceso común y otras vías similares. Por supuesto, el contagio se producía siempre de forma accidental. Las infecciones salían a la luz cuando el virus, tras haber ido trasladándose lentamente de un departamento a otro de la empresa infectando archivos a su paso, era detectado en varios puntos al mismo tiempo por un antivirus actualizado, o se daba a conocer presentando ante el usuario su mensaje de presentación.

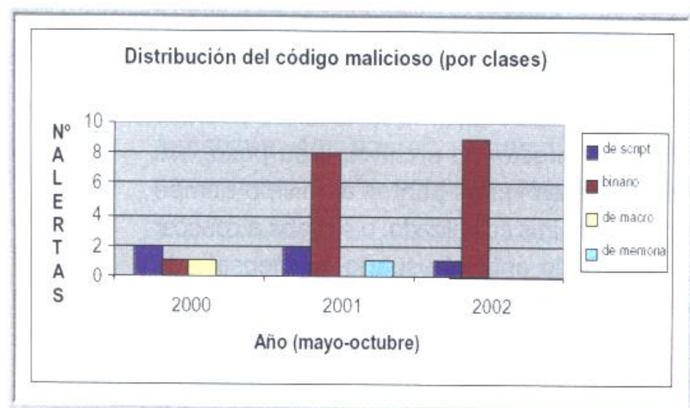
La rápida evolución que han experimentado los gusanos se debe a que los desarrolladores de virus han hallado la manera de propagar sus maliciosas creaciones más rápido y en un mayor número de equipos. Si observamos el mismo periodo de tiempo que teníamos en cuenta hace un momento, veremos que cuatro de cada cinco elementos de código malicioso "en libertad" -in the wild- era un gusano puro. Actualmente, el 100% de los virus detectados presentan

rasgos típicos de los gusanos.

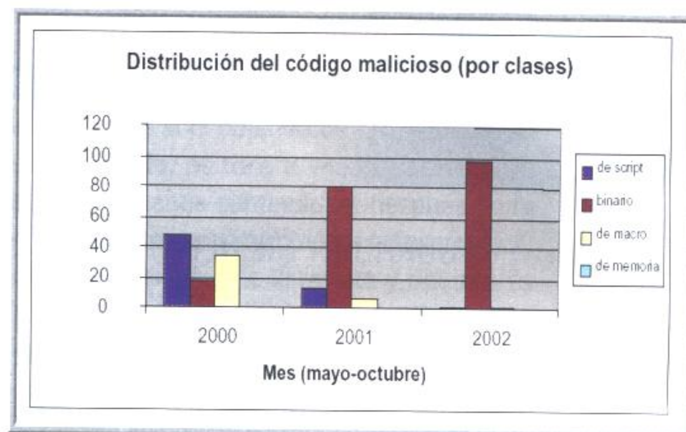
Distribución del código malicioso (difusión)



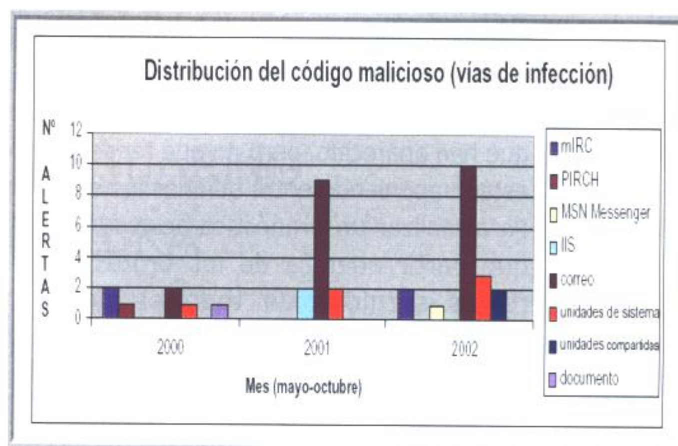
Al examinar más de cerca estos datos, ya desglosados, se advierte que los virus de script y de macro han perdido eficacia, desapareciendo prácticamente del gráfico a principios del año 2002. El siguiente gráfico se ha extraído de estadísticas reales elaboradas en TrendLabs, la red de centros de investigación de Trend Micro Inc.



Si expresamos en un gráfico similar datos recogidos por el equipo de la revista **Virus Bulletin** relativos al mismo periodo de tiempo, se observa que el crecimiento porcentual de código malicioso libre, ¡equivale en número a las alertas víricas documentadas en los tres años!



El panorama actual del código malicioso informático resulta, por sus características, de lo más variopinto. Por un lado, el IRC resurge en el año 2002 como vía de distribución de código malicioso. Al parecer, hay cada vez más interesados en llevar a cabo la hazaña de aprovecharse de las vulnerabilidades de sistema de servicios de publicación de la red como el IIS de Microsoft o Apache, así como desarrolladores de códigos maliciosos "conceptuales" para el servidor SQL de Microsoft. Otra tendencia muy clara es utilizar como medio de difusión los envíos masivos, las unidades compartidas del sistema y la mensajería instantánea (P2P). El término amenaza mixta se ha acuñado para referirse a estos tipos de código malicioso que infectan a través de varias vías al mismo tiempo (ver gráfico siguiente).



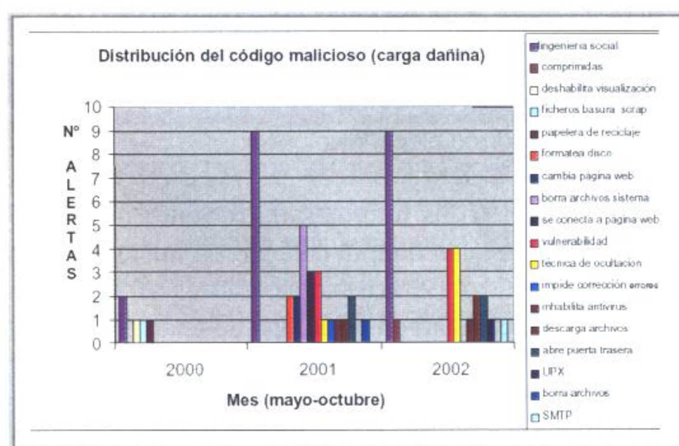
A la hora de concebir estrategias de protección para el futuro, a partir de la información expresada en el gráfico anterior, los administradores deberían tener en cuenta las características particulares que el código malicioso adopta con el fin de sobrevivir cuando penetra en el entorno de una empresa. La mayoría de los gusanos, volviendo al primer gráfico que presentamos, utilizan mensajes de correo electrónico que simulan venir de amigos o conocidos para convencer a quienes los reciben de que pinchen y ejecuten los archivos que vienen adjuntos.

En el cuadro siguiente se ve que, cada vez más a menudo, la autocompresión y el cifrado complican aún más las cosas, al suponer una dificultad añadida a la hora de analizar los efectos negativos de un elemento de código malicioso. Las vulnerabilidades y errores de programas de uso habitual han demostrado ser el talón de Aquiles de las estrategias de protección, pasando por consiguiente a ocupar un lugar destacado en el arsenal de los hackers o piratas informáticos.

Dependiendo del grado de privilegio que se otorgue a los usuarios en un sistema inseguro, los piratas podrán volver a entrar por puertas traseras para seguir haciendo más daño. Los fabricantes de antivirus o de productos de seguridad poco pueden hacer en estos casos, si los programadores no dan con un parche para el software vulnerable o proporcionan enlaces a soluciones externas.

Otra técnica en auge es la de introducir en los equipos código malicioso autoinstalable que atraiga actualizaciones desde sitios Web invadidos por piratas. Un simple enlace unido a código ActiveX puede atravesar tranquilamente el antivirus y el software de filtrado hasta llegar al confiado usuario, que no dudará en hacer doble clic sobre él. Otra característica del código malicioso actual es hacer pruebas de autoconfirmación de su presencia en un sistema, para a continuación deshabilitar y eliminar el antivirus, cortafuegos personal o software antitroyanos que se estén ejecutando en la memoria de la máquina.

5.- Cuando el gran público se estaba acostumbrando a culpar a Outlook y Outlook Express por las infiltraciones que con tanta facilidad sufren, los creadores de virus comienzan a enviar sus desarrollos con su propio protocolo de transporte de correo (SMTP), desvinculándose totalmente de la interfaz de programación de aplicaciones de mensajería (MAPI) que emplean los programas de correo de Microsoft. También los escritores de virus aprenden de sus errores y están regresando a los virus en estado puro, eliminando las cargas dañinas. Esta impresión se obtiene al comparar los datos de 2001 con los del 2002, todos en el gráfico siguiente.



Lo importante ahora es saber qué nos espera. De los hechos observados y presentados se infieren claramente los siguientes pronósticos y estrategias, que se irán manifestando a medida que nos adentremos en el 2003:

* La norma seguirá siendo que las redes se vean acechadas por amenazas mixtas.

* El código malicioso actual y el que se cree en el futuro intentará por distintos medios deshabilitar los programas antivirus, cortafuegos personales o incluso antitroyanos que protejan los sistemas.

* Habrá que instalar en las empresas software de filtrado de páginas Web o, por lo menos, aplicar medidas que impidan que los usuarios sean redireccionados sin darse cuenta a sitios de Internet que contengan código malicioso.

* Como medida de protección extra seguirán filtrándose los archivos adjuntos a los mensajes de correo. No obstante, los antivirus ubicados en la pasarela de Internet serán más eficaces a la hora de evitar que archivos infectados se cuelen en las redes de las empresas.

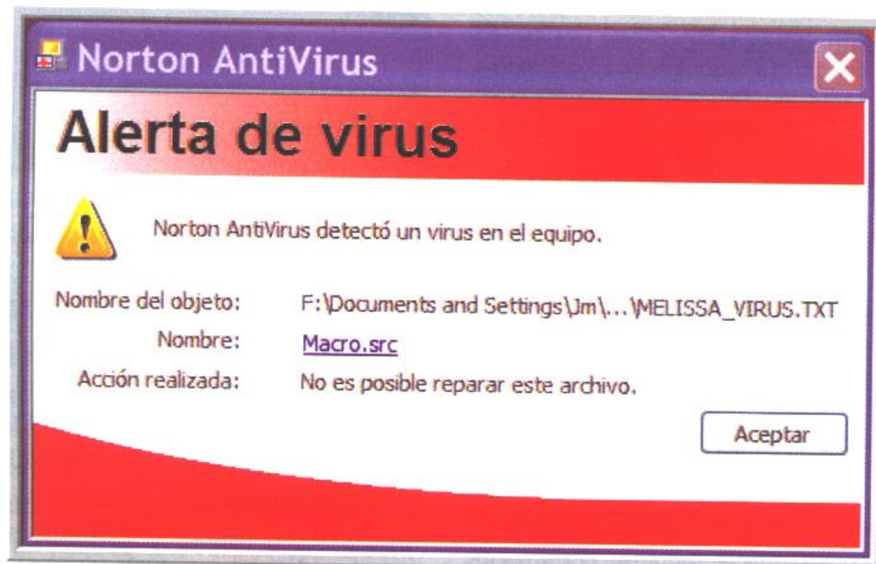
* Se recurrirá de cuando en cuando a los tan extendidos canales públicos de mensajería, como el IRC y los P2P, dada la explosión que experimentará la demanda de comunicaciones más rápidas. Sin embargo, la actividad cotidiana en las empresas seguirá lastrada por un sobrecargadísimo volumen de correo electrónico.

* Varios informes de reciente publicación señalan que, al parecer, en menos de cinco años, el 25% del correo electrónico que circulará consistirá en algún tipo de texto promocional no solicitado: dos de cada diez mensajes que entran en los buzones personales.

* Microsoft está apostando fuerte por su plataforma .NET prometiendo que crecerá en muy poco tiempo y que será muy sencilla de integrar en un amplio abanico de dispositivos informáticos. Hasta el momento, ha habido cuatro intentos de crear código malicioso para este nuevo medio, lo que resulta preocupante puesto que, en caso de hacerse realidad, sería código dañino capaz de penetrar en todas las plataformas que admitiesen esta arquitectura.

* Los administradores de sistema deben evaluar cuidadosamente las necesidades de sus redes en términos de software y elegir programas cuyos desarrolladores puedan comprometerse como mínimo a aportar remedios a las vulnerabilidades que puedan encontrarse antes de que sea demasiado tarde. Ningún fabricante puede afirmar que su software, aunque ha pasado pruebas exhaustivas, funcionará siempre perfectamente.

Por consiguiente, al prepararse para defender mejor las redes que tienen a su cargo, los administradores deberán buscar productos y servicios que ofrezcan, con total seguridad y continuidad en el tiempo,soluciones adecuadas a los problemas que acabamos de plantear.



OCULTACION DE FICHEROS: METODO STREAM (ADS)

Con este artículo te enseñaremos, por ejemplo, a ESCONDER un video de 600 MB en un fichero de texto de CERO KB SIN utilizar virus, rootkits, modificaciones del kernel, u otros agentes infecciosos. ¿No te lo crees? Pues PREPÁRATE, ni siquiera un administrador experimentado encontrará estos archivos ocultos.

1.- Para los incrédulos:

En Hack x Crack hemos explicado muchas veces lo importante que es conocer las diferencias entre un programa (el código) y la interfaz gráfica de ese programa (las ventanitas). Juntos hemos aprendido que una simple línea de comandos es más poderosa que la más compleja de las interfaces gráficas, hemos demostrado que una ventanita NUNCA puede explotar a fondo las posibilidades reales de un programa.

Creo que fue en Hack x Crack número 1 cuando dijimos que os explicaríamos la ocultación avanzada de ficheros, pues ha llegado el momento!!! No solo vamos a demostrarte una vez más que la interfaz gráfica de WINDOWS te ofrece un mísero control sobre el Sistema Operativo, te demostraremos que MICROSOFT OCULTA ¿INTENCIONADAMENTE? Los comandos que podemos utilizar para administrar nuestros sistemas.

Todo esto no tendría mayor trascendencia si no fuese porque supone dejar a un ADMINISTRADOR INDEFENSO ante su propio S.O. (Sistema Operativo), no importa cuántos años has dedicado a estudiar informática, no importa cuántos años de experiencia tengas: MICROSOFT DECIDE LO QUE TU NO DEBES SABER.

2.- ALTERNATE DATA STREAM (ADS)

La serie Windows NT (NT, 2000 y XP) nos ofrece la posibilidad de instalar en Sistema Operativo en un Sistema de Ficheros llamado NTFS.



Un sistema...

Un sistema de ficheros "simplemente" es la forma en que un Sistema Operativo "maneja" los archivos en tu disco duro. En el caso de la serie Windows 9x (95, 98 y ME) se utilizaron los conocidos FAT16 y FAT32 y en la serie Windows NT (NT, 2000 y XP) se utiliza NTFS. NTFS es mucho más seguro y versátil (podemos crear políticas de acceso a nuestros ficheros, cifrar nuestras carpetas, etc.).

El sistema NTFS tiene una "capacidad" NO DOCUMENTADA que nos permite utilizar los llamados Alternate Data Stream (ADS). Esta "capacidad" nos permite asociar "información" a un archivo (e incluso a un directorio) y existe para mantener una cierta compatibilidad con el HFS (Sistema de Archivos de Macintosh, Hierarchical File System).

Cuando asociamos un archivo1 a un archivo2, el archivo2 permanece invariable PERO "contiene" el archivo1 "en su interior". El archivo1 queda ocultado a nuestro querido Windows pero sigue existiendo e incluso en caso de ser un ejecutable PUEDE SER

EJECUTADO!!! Empieza a imaginar lo que podría hacer un virus... ...



Los virus...

Los virus actualmente NO UTILIZAN esta técnica, pero existen estudios que aseguran que el presente año (2003) será el año de los virus-stream. Esperemos que los antivirus empiecen a estudiar cómo detener estos "monstruos", porque la carrera ya ha empezado, un ejemplo son las recientes "creaciones" del grupo 29ª (por ejemplo el virus W2Kstreams).



Debes realizar...

Para realizar las prácticas que a continuación detallaremos DEBES tener instalado un Windows de la serie NT (NT, 2000 o XP) sobre el Sistema de Archivos NTFS de Microsoft. Actualmente Windows XP se instala de esta forma por defecto y cualquier Servidor de Internet basado en Windows es instalado de esta forma.

3.- ¿Tengo yo mi "querido" Windows montado en una partición NTFS?

Para comprobar si tu configuración es la correcta y para ir "tomando contacto" abriremos una Ventana de Comandos (Menú Inicio --> Ejecutar, escribimos cmd.exe y pulsamos aceptar).





Nos hemos...

Nos hemos cansado en números anteriores de explicar cómo abrir una Ventana de Comandos, si tienes dudas, recuerda que puedes descargar el número uno de PC PASO A PASO (Hack x Crack) desde nuestra Web (www.hackxcrack.com).

Introduciendo el comando chkdsk y pulsando enter veremos como lo primero que sale es un mensaje indicándonos nuestro Sistema de Archivos (NTFS en nuestro caso) y de paso nos chequeará el Disco Duro buscando errores :)



4.- La práctica (primera parte)

Para crear un fichero "oculto" (lo llamaremos fichoc.txt) dentro de otro (lo llamaremos fichreal.txt) simplemente tenemos que añadir dos puntos ":" y un nombre a la derecha del fichero "troyanizado" (fichreal.txt).

A) Vamos allá, crearemos una carpeta cualquiera (nosotros la llamaremos hxcads) en c:\ y nos metemos dentro.

1.- Vamos al directorio raíz del sistema c:\ escribiendo

cd\ (y pulsamos enter)

2.- Creamos el directorio hxcads escribiendo

md hxcads (y pulsaremos enter)

3.- Nos metemos dentro de la carpeta escribiendo

cd hxcads (y pulsaremos enter)

```
C:\WINDOWS\System32\cmd.exe
C:\Documents and Settings\RUBEN>cd\
C:\>md hxcads
C:\>cd hxcads
C:\hxcads>
```

B) Ahora crearemos un fichero de texto llamado fichreal.txt y su contenido será el mensaje "Este es un fichero visible", escribiremos

-echo este es un fichero visible>fichreal.txt (y pulsaremos enter)

Podemos hacer un dir veremos que el fichero de texto fichreal.txt ha sido creado.

```
C:\WINDOWS\System32\cmd.exe
C:\hxcads>echo este es un fichero visible>fichreal.txt

C:\hxcads>dir
 El volumen de la unidad C no tiene etiqueta.
 El número de serie del volumen es: 1871-9F3A

 Directorio de C:\hxcads

16/01/2003  04:17    <DIR>          .
16/01/2003  04:17    <DIR>          ..
16/01/2003  04:17                28 fichreal.txt
               1 archivos             28 bytes
               2 dirs  23.493.304.320 bytes libres

C:\hxcads>
```

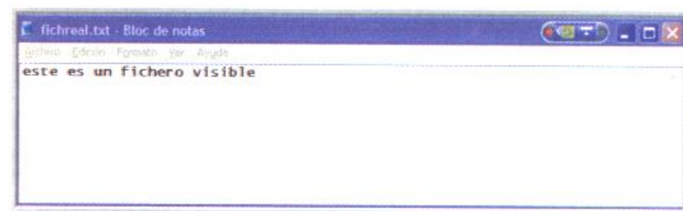


echo junto a...

echo junto a > mete "lo que sea dentro de el fichero, si este fichero no está creado, lo crea.

Fíjate bien que el archivo fichreal.txt "pesa" 28 bytes y recuérdalo ;p

Podemos abrir este archivo con el Bloc de Notas (notepad) para que realmente su contenido es la frase "este es un fichero visible"





Ya hemos...

Ya hemos trabajado en anteriores números con el comando echo y el comando dir.

C) Ahora crearemos un fichero de texto llamado fichoc.txt con el texto "este archivo está oculto" y lo "esconderemos" dentro de fichreal.txt :)

1.- Creamos el fichero de texto fichoc.txt con el contenido "este archivo esta oculto", escribiendo

echo este archivo esta oculto >fichoc.txt (y pulsaremos enter)

2.- Utilizamos por primera vez el "efecto stream" ;) Metemos el fichero fichoc.txt dentro del fichero del fichero fichreal.txt, escribiendo

type fichoc.txt>fichreal.txt:oculto

3.- Ahora eliminamos el fichero fichoc.txt puesto que ya lo hemos "introducido" dentro de fichreal.txt, escribiendo

del fichoc.txt

4.- Finalmente hacemos un dir para ver que realmente hemos borrado el archivo fichoc.txt y solo nos queda el fichero fichreal.txt, escribiendo

dir

```
C:\WINDOWS\System32\cmd.exe
C:\hxcads>echo este archivo esta oculto >fichoc.txt

C:\hxcads>type fichoc.txt>fichreal.txt:oculto

C:\hxcads>del fichoc.txt

C:\hxcads>dir
 El volumen de la unidad C no tiene etiqueta.
 El número de serie del volumen es: 1871-9F3A

 Directorio de C:\hxcads

16/01/2003  04:42    <DIR>          .
16/01/2003  04:42    <DIR>          ..
16/01/2003  04:40                28 fichreal.txt
               1 archivos             28 bytes
               2 dirs  23.490.818.048 bytes libres

C:\hxcads>
```



Fijate bien...

Fíjate bien que el archivo fichreal.txt "pesa" 28 bytes, parece que no ha pasado nada ¿verdad?, todo está como antes ¿no?

Ahora abre el archivo fichreal con el Bloque de Notas (notepad) tal como hicimos antes y verás que no ha cambiado en absoluto :)



Hay otra forma de visualizar del archivo fichreal.txt sin utilizar el Bloque de Notas, mediante el comando more por línea de comandos. Veremos el contenido del fichero, en este caso la frase "este es un fichero visible". Venga, vamos a hacerlo, escribimos

more < fichreal.txt

```
C:\WINDOWS\System32\cmd.exe
C:\hxcads>type fichoc.txt>fichreal.txt:oculto

C:\hxcads>del fichoc.txt

C:\hxcads>dir
 El volumen de la unidad C no tiene etiqueta.
 El número de serie del volumen es: 1871-9F3A

 Directorio de C:\hxcads

16/01/2003  04:42    <DIR>          .
16/01/2003  04:42    <DIR>          ..
16/01/2003  04:40                28 fichreal.txt
               1 archivos             28 bytes
               2 dirs  23.490.818.048 bytes libres

C:\hxcads>more < fichreal.txt
este es un fichero visible

C:\hxcads>
```



"more" es...

"more" es un comando que MUESTRA INFORMACIÓN. En este caso, junto al símbolo <, lo que hace es EXTRAER (mostrar) en la ventana el fichero fichreal.txt

Si quisiésemos imprimir el fichero fichreal.txt podríamos hacerlo escribiendo

more fichreal.txt>prn (printer)

D) Ha llegado el momento!!! Vamos a visualizar el contenido del fichero fichoc.txt (el que hemos ocultado dentro de fichreal.txt). Lo haremos escribiendo

more < fichreal.txt:oculto

Y obtenemos la frase este archivo está oculto, es decir, el contenido del fichero fichoc.txt :) ¿Cómo se te ha quedado el cuerpo? Fíjate bien que el archivo fichreal.txt NO HA CAMBIADO en absoluto, ocupa lo mismo (28 bytes) y tanto si lo abres con el Bloque de Notas como con el comando more (por línea de comandos) ves su contenido inicial (el texto "este es un fichero visible").

```
C:\WINDOWS\System32\cmd.exe
C:\hxcads>del fichoc.txt

C:\hxcads>dir
 El volumen de la unidad C no tiene etiqueta.
 El número de serie del volumen es: 1871-9F3A

 Directorio de C:\hxcads

16/01/2003  04:42    <DIR>          .
16/01/2003  04:42    <DIR>          ..
16/01/2003  04:40                28 fichreal.txt
               1 archivos             28 bytes
               2 dirs  23.490.818.048 bytes libres

C:\hxcads>more < fichreal.txt
este es un fichero visible

C:\hxcads>more < fichreal.txt:oculto
este archivo esta oculto

C:\hxcads>_
```



Vamos a hacer...

Vamos a hacer un paréntesis :), que te veo "ofuscado".

5.- ¿Qué ha pasado realmente?

Lo que ha pasado es que hemos ASOCIADO el contenido del archivo fichoc.txt al archivo fichreal.txt mediante "stream". Cuando hacemos esto el contenido del archivo asociado (fichoc.txt) queda "oculto" dentro del fichero "troyanizado" (el fichreal.txt) y para colmo, el fichero troyanizado sería capaz de pasar un test byte a byte (o un test de CRC, o un test de un antivirus) porque NO HA SIDO MODIFICADO.

Vamos a ver si ampliando el ejemplo mejoramos nuestra visión del tema.

6.- La práctica (segunda parte)

No toques nada!!! Vamos a ocultar un archivo de música o video dentro del archivo fichreal.txt Y VAMOS A EJECUTARLO!!! ¿no te lo crees?

A) Copiamos un archivo de música o de video en la carpeta hxcads, nosotros hemos copiado un video de nombre blake.avi que no es ni más ni menos que un video de Andrew Blake que "pesa" la friolera de 710 Megas. ¿Cómo? ¿Que no sabes quién es Andrew Blake? Bueno, eso dejaremos que lo averigües tu solito ;p

```
C:\WINDOWS\System32\cmd.exe
C:\hxcads>dir
 El volumen de la unidad C no tiene etiqueta.
 El número de serie del volumen es: 1871-9F3A

 Directorio de C:\hxcads

16/01/2003  05:54    <DIR>          .
16/01/2003  05:54    <DIR>          ..
20/12/2002  13:41       727.310.336 blake.avi
16/01/2003  04:40                28 fichreal.txt
               2 archivos    727.310.364 bytes
               2 dirs  22.757.765.120 bytes libres

C:\hxcads>
```

B) Hacemos "streaming", es decir, "metemos" el fichero blake.avi dentro del fichero fichreal.txt, escribiendo

type blake.avi>fichreal.txt:oculto2.avi

C) Borramos el archivo blake.avi escribiendo del blake.avi

D) Hacemos un dir para ver que realmente solo nos hemos quedado con el fichero fichreal.txt



Fijate bien...

Fíjate bien que nuestro archivo fichreal.txt NO HA CAMBIADO!!! Puedes abrirlo como hicimos antes (Bloque de Notas o comando more) o simplemente ver que sigue ocupando lo mismo: 28 bytes :)

E) Ahora VAMOS A EJECUTAR (VISUALIZAR) NUESTRO VIDEO!!!, tan solo tienes que escribir

start .\fichreal.txt:oculto2.avi

En este momento se abrirá nuestro visualizador de videos (en nuestro caso el Windows Media Player) y reproducirá la película :)



Vamos a hacer...

Esto lo conseguimos utilizando el comando start.

7.- Sala de preguntas:

A) Seguro que te estás preguntando dónde demonios ha ido a parar un fichero avi de 700MB!!! Pues bien, toda la información que había en el fichero AVI (los 700MB) SI EXISTEN, están asociados al archivo fichreal.txt; PERO tu querido Windows no tiene las herramientas necesarias para trabajar correctamente con ellos, simplemente NO PUEDES verlos y punto!!! Ni tu ni nadie puede verlos, si no sabes que están ahí, nunca podrás acceder a ellos, así de claro y así de duro :)

Seguramente ya sabes lo que supone eso ¿verdad? Ahora mismo se me ocurren mil cosas

que hacer con este regalo de Microsoft, y casi todas malas. Lo peor de todo es la indefensión de un administrador frente a esta situación, porque si alguien te entra en un servidor y utiliza esta técnica, BOOOOOM... se acabó el juego!!!!

B) Otra preguntita que los espabilados deben estar haciéndose. Hemos ocultado dos archivos dentro de un mismo archivo, ¿es esto posible?

Si, perfectamente posible. Un mismo archivo (en nuestro caso un mísero TXT de 28 bytes) puede "contener" varias "asociaciones", en nuestro caso una de ellas era de 700MB!!!

C) Hay algo que no me queda claro, a ver si me iluminas. En el primer caso, has metido el archivo fichoc.txt dentro del fichreal.txt y lo has visualizado con el comando more, ¿verdad? Bien, pues yo he intentado "ejecutar" (visualizar) el archivo fichoc.txt igual que has hecho con el video Y NO PUEDO!!! ¿Qué pasa? He utilizado la línea

start .\fichreal.txt:oculto

Vamos por partes. Cuando hemos metido el fichoc.txt dentro del fichreal.txt hemos utilizado la línea type fichoc.txt>fichreal.txt:oculto. Lo que debemos tener en cuenta es que, lo que hay a la derecha de los dos puntos (en este caso "oculto") será el nuevo nombre del fichero fichoc.txt. Nosotros lo llamamos NOMBRE ASOCIADO.

Fíjate que el nombre "oculto" no tiene extensión, por eso Windows no es capaz de abrirlo directamente. Para que Windows lo abriese directamente tendríamos que ábrelo "ocultado" con el nombre oculto.txt, de esa forma, escribiendo la línea

start .\fichreal.txt:oculto.txt

nuestro Windows habría sabido que era un fichero de texto y lo habría abierto con el Bloc de Notas

Fíjate que el video blake.avi lo hemos ocultado como con el NOMBRE ASOCIADO oculto2.avi (extensión AVI), por eso al ejecutarlo (visualizarlo) con el comando start, nuestro Windows ha abierto nuestro reproductor de "pelis".

D) Eso significa que si ocultase un ejecutable (por ejemplo un troyano.exe) ¿se podría ejecutar con el comando start?

Por supuesto!!!!!!!!!, después te pongo un ejemplo :)

E) Pero... ¿no hay manera de "controlar" este AGUJERO SIN FONDO?!!! No puede ser, debe haber alguna manera de poder controlar todo esto.

Pues sí, con un poco de ayuda de programas externos, después te los presento ;)

8.- La práctica (tercera parte)

Vamos a esconder un ejecutable (*.exe) dentro de nuestro fichreal.txt y a ejecutarlo.

A) Copiamos un ejecutable en nuestra carpeta c:\hxcads, nosotros hemos copiado el fichero calc.exe (la calculadora de Windows).



El archivo...

El archivo calc.exe lo encontrarás en c:\windows\system32 en caso de tener el Windows XP.

B) Escondemos el fichero calc.exe dentro de nuestro fichreal.txt dándole como NOMBRE ASOCIADO calculator.exe :), escribiendo

type calc.exe>fichreal.txt:calculator.exe

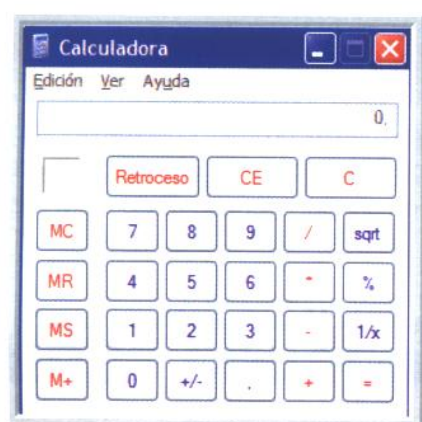
C) Borramos el fichero calc.exe escribiendo del calc.exe

D) Ejecutamos el fichero "escondido" llamado

calculator.exe escribiendo
start .\fichreal.txt:calculator.exe

```
C:\WINDOWS\System32\cmd.exe
C:\hxcads>type calc.exe>fichreal.txt:calculator.exe
C:\hxcads>del calc.exe
C:\hxcads>start .\fichreal.txt:calculator.exe
C:\hxcads>
```

y se nos abrirá la calculadora de Windows :)





Fíjate bien...

Fíjate bien que, al igual que con el video, hemos borrado el archivo ocultado (en este caso el calc.exe). Es importante que no confundas las cosas, este método NO CREA una asociación entre el fichero original (calc.exe) y el "troyanizado" (fichreal.txt). Este método realmente mete el código del calc.exe "dentro" de nuestro inocente fichreal.txt. El problema es que Windows ES INCAPAZ de mostrártelo :)

9.- La práctica (cuarta parte): TROYANIZANDO ARCHIVOS DE WINDOWS

No hace falta decirte que puedes hacer esto con cualquier archivo del sistema. Me explico, hasta el momento nosotros hemos creado un fichero llamado fichreal.txt y hemos escondido dentro otros ficheros.

Si quieres, puedes hacer lo mismo con cualquier archivo, puedes meter cualquier fichero dentro de cualquier fichero, un exe dentro de un doc o un txt dentro de un avi o... ... y por supuesto, puedes meter CUALQUIER TIPO DE "BICHO"dentro de cualquier archivo del sistema (por ejemplo dentro de una dll) y hacer cualquier cosa que se te ocurra.

10.- La práctica (quinta parte): TROYANIZANDO un directorio.

Muy interesante esta posibilidad :) No necesitas un archivo para esconder ficheros por el método "stream", PUEDES TROYANIZAR un simple directorio (cualquier carpeta de tu querido Windows).

A) Creamos un directorio cualquiera, por ejemplo c:\hxc10, escribiendo

cd\ --> nos vamos al directorio raíz
md hxc10 --> creamos el directorio c:\hxc
cd hxc10 --> entramos en la carpeta

B) Vamos a "esconder" (asociar) la calculadora de Windows (calc.exe) dentro de la carpeta c:\hxc10, escribiendo

Type c:\windows\system32\calc.exe > :calculadora.exe



Acabamos de...

Acabamos de hacer un stream a la propia carpeta, no a un fichero, por eso no hay ningún nombre a la izquierda de los dos puntos ":"

C) Hacemos un dir y vemos que realmente la carpeta hxc10 no contiene ningún archivo, recuerda que hemos hecho un stream a la propia carpeta :)

dir

```
C:\WINDOWS\System32\cmd.exe
C:\>cd\

C:\>md hxc10

C:\>cd hxc10

C:\hxc10>type c:\windows\system32\calc.exe > :calculadora.exe

C:\hxc10>dir
 El volumen de la unidad C no tiene etiqueta.
 El número de serie del volumen es: 1871-9F3A

 Directorio de C:\hxc10

16/01/2003  17:31    <DIR>          .
16/01/2003  17:31    <DIR>          ..
               0 archivos              0 bytes
               2 dirs  22.014.410.752 bytes libres

C:\hxc10>
```



Para poder...

Para poder hacer esto, tenemos que estar dentro de la carpeta que queremos "troyanizar". Fíjate bien que en el apartado A) hemos entrado en la carpeta hxc10 mediante la línea "cd hxc10 --> entramos en la carpeta"

11.- La práctica (sexta parte): Un directorio de texto de tamaño CERO!!! Que puede contener "lo que tu quieras".

Para crear un fichero de texto de tamaño cero y que contenga un mensaje oculto podemos hacerlo escribiendo

Echo esto es un mensaje oculto > mensaje.txt:megusta

Hacemos un dir para ver que realmente tenemos un archivo de texto de tamaño cero :)

```
C:\WINDOWS\System32\cmd.exe
C:\hxc10>Echo esto es un mensaje oculto > mensaje.txt:megusta

C:\hxc10>dir
 El volumen de la unidad C no tiene etiqueta.
 El número de serie del volumen es: 1871-9F3A

 Directorio de C:\hxc10

16/01/2003  18:14    <DIR>          .
16/01/2003  18:14    <DIR>          ..
16/01/2003  18:14                 0 mensaje.txt
               1 archivos              0 bytes
               2 dirs  22.004.924.416 bytes libres

C:\hxc10>
```

Si abrimos el archivo mensaje.txt con el Bloc de notas, veremos que es un fichero de texto completamente vacío. PERO si visualizamos el mensaje introducido por "streamer" (NOMBRE ASOCIADO "megusta") mediante el comando more, veremos nuestro mensaje oculto :)

More < mensaje.txt:megusta

```
C:\WINDOWS\System32\cmd.exe
C:\hxc10>dir
 El volumen de la unidad C no tiene etiqueta.
 El número de serie del volumen es: 1871-9F3A

 Directorio de C:\hxc10

16/01/2003  18:14    <DIR>          .
16/01/2003  18:14    <DIR>          ..
16/01/2003  18:14    .            0 mensaje.txt
               1 archivos              0 bytes
               2 dirs  22.004.924.416 bytes libres

C:\hxc10>More < mensaje.txt:megusta
esto es un mensaje oculto

C:\hxc10>
```

Ahora podríamos dedicarnos a troyanizar este inofensivo archivo de texto de tamaño cero como hemos hecho hasta ahora, pudiendo meter dentro, no se... por ejemplo ¿3GB de Warez? :p

12.- La práctica (séptima parte): Ejecución de scripts.

Dentro de muy poco explicaremos eso de los scripts en el curso de programación, por ahora simplemente piensa que son instrucciones (o conjunto de instrucciones) que realizan tareas concretas, parecido a un *.EXE (vale, vale, no es un exe... lo he descrito así para que todos nos entendamos :)

Por ejemplo, escribe
Echo MsgBox "Mensaje y saludo en Visual Basic" > hola.txt:saludo.vbs

Y ahora ejecutamos el saludo.vbs, que está oculto dentro de hola.txt, escribimos

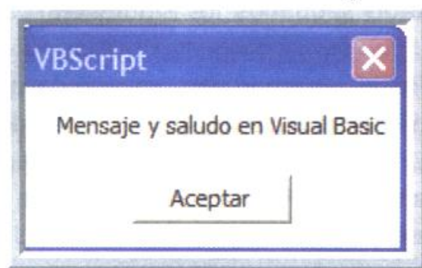
Start .\hola.txt:saludo.vbs

```
C:\WINDOWS\System32\cmd.exe
C:\hxc10>Echo MsgBox "Mensaje y saludo en Visual Basic" > hola.txt:saludo.vbs

C:\hxc10>Start .\hola.txt:saludo.vbs

C:\hxc10>
```

Veremos como aparece una ventana en la pantalla dándonos un saludo!!! ;)





Si no sabes...

Si no sabes lo que es la "instrucción" MsgBox, no te preocupes, ya lo aprenderemos juntos en el curso de Visual Basic ;)

13.- Software para "ver" los STREAMS.

La herramienta más sencilla para "ver" los streams es LADS de http://www.heysoft.de Para utilizarla tan solo debes copiar el archivo lads.exe dentro del directorio que quieras examinar y ejecutarla por linea de comandos, escribiendo

lads



Hay más que explicar, pero nos quedamos sin espacio por este mes.

TRASTEANDO CON EL HARDWARE DE UNA LAN.

POR JOSÉ L. VIZCAÍNO.

Muchas empresas tienen instalados unos clientes de red que se encargan de gestionar y controlar los accesos de los empleados, dada las pocas ganas de complicarse y los bajos conocimientos de hardware que tienen algunos administradores vemos como cada ordenador-terminal que corre bajo sistema operativo Windows tiene unos agujeros que podemos intentar utilizar.

Aunque a veces hemos visto como se hace necesario el uso de la ingeniería social para poder introducirnos en algún sistema de estas características, hoy vamos a ver otro tipo de método: vamos a utilizar unas pequeñas nociones de Hardware, de Windows y el uso de un Keylogger.

Este tipo de trucos funciona principalmente en redes LAN con algún tipo de cliente de red, tipo Novell Netware, que requiera la identificación para entrar en ella y con el S.O. Windows instalado en cada una de las estaciones de trabajo (vamos a ir a lo mas común; para otro tipo de Netware y de S.O. el modo puede variar, pero conociéndolos de antemano es muy posible que puedas hacer algo igual).

Primer Problema, muy sencillo y lógico: Vamos a escribir una carta y la vamos a imprimir desde un terminal cualquiera de la red.

Arrancamos el ordenador y dejamos que cargue Windows hasta que nos encontremos con la ventana de identificación para el acceso a la red y pulsamos CANCELAR, vemos como Windows continua con el proceso de arranque y pone a nuestra disposición todo el ordenador (que no es poco). Una vez que veamos el escritorio nos levantamos y damos una vuelta alrededor del ordenador para revisar las conexiones, sobre todo buscamos saber si tiene una impresora conectada y dependiendo del resultado seguimos los siguientes pasos:

1º- Tiene una impresora conectada por el Puerto Paralelo o USB... entonces la encendemos (así ya la tenemos iniciada para cuando la necesitemos). Ahora debemos saber si la impresora esta configurada para ser utilizada como impresora de red o como impresora local, para ello seguimos la siguiente ruta dentro del escritorio:

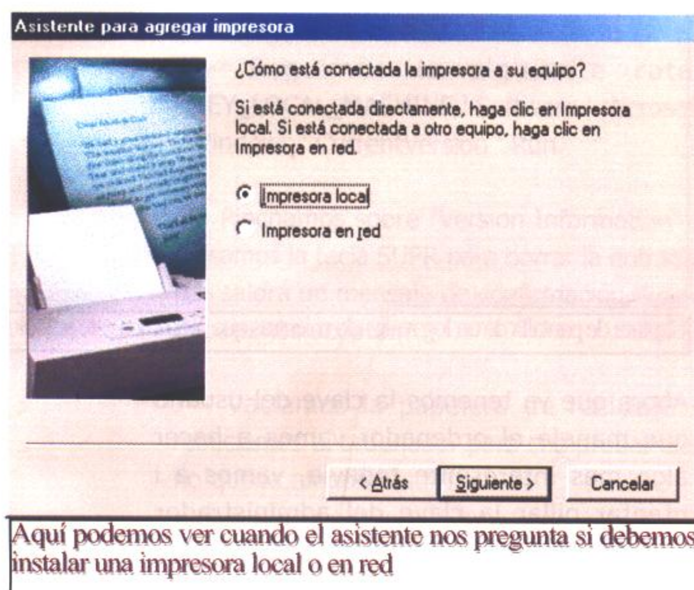
INICIO ' CONFIGURACION 'PANEL DE CONTROL ' IMPRESORAS

Nos saldrán varios iconos, el primero "AGREGAR IMPRESORA" (que veremos más adelante para que nos puede servir) y los demás iconos son de las impresoras que están instaladas en el ordenador. Buscamos el icono de la impresora (que coincida con la marca y el modelo) y el mismo icono nos dirá si esta instalada en red o local dependiendo de si tiene una especie de T invertida de color amarillo en su parte inferior.

Supuesto 1º: La impresora esta como local, entonces abrimos el wordpad escribimos la carta y le damos a imprimir.... ¡ya esta!, preocúpate de eliminar el archivo (incluso de la papelera de reciclaje) y dejar todo como estaba para que nadie se de cuenta.

Supuesto 2º: La impresora esta en red y, como no podemos acceder a ella, no nos deja imprimir, pues vamos a utilizar el ingenio, volvemos a la carpeta "IMPRESORAS" y pinchamos sobre el icono "AGREGAR IMPRESORA", entonces empezará el asistente para instalar una impresora, seleccionamos que es una impresora local, la marca y el modelo y ... ¿y los drivers?... no hay problema, el ordenador ya los tiene, lo único que hará será "cambiarlos de lugar", al final del proceso veremos como tiene dos iconos de impresoras instaladas, ambas la misma marca y modelo

pero una en red y otra en modo local... ahora seguimos los pasos del supuesto 1º y a la hora de imprimir (en el menú de impresión) seleccionamos la impresora que está como local y ya está hecho... después asegúrate de borrar el icono que has creado y de no dejar nada en la papelera de reciclaje no sea que alguien se de cuenta...



Aquí podemos ver cuando el asistente nos pregunta si debemos instalar una impresora local o en red

Supuesto 3º: No hay ninguna impresora conectada. Volvemos a la carpeta de impresoras y averiguamos cuales son las impresoras que tiene instaladas en red, cuando lo sepamos tenemos que localizar donde están físicamente y seleccionar la mas cercana (para evitar que nadie te vea), la desconectamos del PC al que este acoplada y la acoplamos al "nuestro", después tenemos que seguir los pasos del Supuesto 2º, y, al acabar, dejar todo en su sitio...

Esta es una pequeña demostración de como con un poco de ingenio podemos arreglarnos para hacer alguna cosilla sin tener conocimientos de casi nada... pero esto es solo un avance; ahora vamos a ver otro problemilla mas serio pero no menos fácil de solucionar.

Segundo Problema: Vamos a escribir imprimir en red (por hacerlo más difícil ya que tenemos tiempo) o vamos a navegar por Internet o vamos a hacer lo que nos de la gana pero entrando dentro de la red.

Vamos a intentar entrar en la red, pero para ello necesitamos las claves de uno o varios usuarios, normalmente cada clave da acceso a unas herramientas y archivos dependiendo que quien sea, esto quiere decir que todos no tendrán acceso a los mismos archivos o programas aunque varios de ellos puedan compartirlos.

1º Método: La Ingeniería Social: Intenta ingeniártelas para que alguien te pase su clave (¿difícil verdad?) aunque en empresas grandes en las que no se conocen entre ellos puede funcionar haciéndote pasar por alguien del departamento de informática.

2º Método: Mediante los archivos PWL de Windows, pero para ello necesitaras que estén bien configuradas las contraseñas de Windows (algo casi imposible), que estas sean las mismas que las de acceso a la red y un programa que desencripte las claves que tendrás que introducir en el sistema.

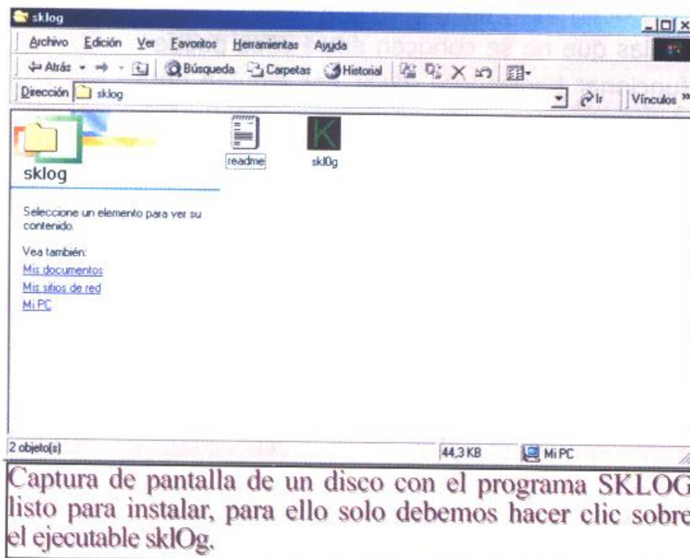
3º Método: Utilizando Keyloggers para capturar las contraseñas de los usuarios: Que es mi opción preferida porque requiere menos conocimientos de "hacking" y, en el peor de los casos, el uso de la lógica del Hardware.

EXPLICACION DEL METODO. (Con una simple disquetera de 3 ½ Interna.)

Si el ordenador tiene disquetera, el siguiente paso es instalar un Keylogger. En este caso he elegido el SKLOG, un anónimo Keylogger de muy pocas Kbs. pero que captura las teclas tal y como se pulsan. Además esta muy bien

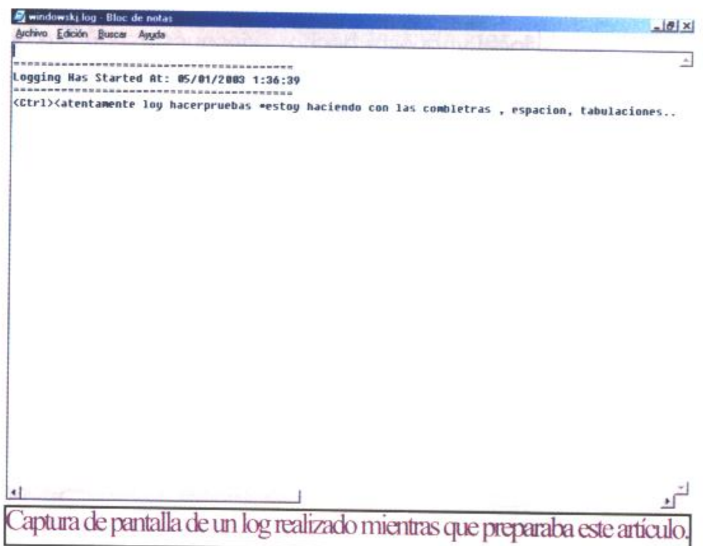
camuflado, se oculta identificándose como el programa "winsystem" por lo que, si no conoces realmente cual es ese programa, no lo te arriesgas a cerrarlo. Además, el SKLOG crea una entrada en el registro del sistema, con lo que, cada vez que alguien arranque el ordenador comenzará a funcionar solo.

Para ello debemos dejar que el ordenador arranque cancelando cualquier ventana que solicite el "Usuario/Clave" hasta que lleguemos al sistema operativo. Metemos el disquete que contenga el SKLOG y vamos a la unidad a:, una vez allí hacemos doble clic sobre el ejecutable SKLOG, el malicioso programa se instalara en nuestra victima, una vez hecho esto solo debemos de esperar un día o dos.



Captura de pantalla de un disco con el programa SKLOG listo para instalar, para ello solo debemos hacer clic sobre el ejecutable sklOg.

El SKLOG guardara en un archivo disponible en c:/windows/system/windowskj.log (en este momento lo tengo instalado y esta registrando todo lo que pongo en todas las ventanas que tengo abiertas), para abrir este archivo debes utilizar el Bloc de Notas o WordPad de Windows; este archivo te mostrará la fecha, la hora y las teclas que se pulsan, hay que tener en cuenta que, cuando se trabaja en una red local protegida con contraseñas, las primeras teclas que se pulsan son las correspondientes al Usuario y la Contraseña, así que solo deberemos leer atentamente las primeras letras y hacer pruebas. Darás con la clave antes de lo que crees.



Captura de pantalla de un log realizado mientras que preparaba este artículo.

Ahora que ya tenemos la clave del usuario que maneja el ordenador vamos a hacer algo mas interesante todavía, vamos a i ntentar pillar la clave del administrador (o alguien con privilegios bastante similares), para ello solo vamos a borrar en el escritorio un acceso directo a un programa muy usado tal como el Word (normalmente quien instala los programas es el administrador o algún similar); cuando el usuario habitual del ordenador descubra que no tiene su procesador de textos llamará al administrador para que se lo reinstale, para ello el tendrá que reiniciar el ordenador y volver a entrar con su usuario y contraseña... que nuestro amigo guardará para nosotros... ahora ya tenemos la contraseña del administrador... imaginaos todo lo que se puede llegar a hacer con ella.

Una vez que ya hemos acabado nuestra experiencia debemos dejar todo como estaba, para borrar el SKLOG debemos seguir los siguientes pasos:

1º- Encender el ordenador y dejar el escritorio (sin entrar en la red).

2º- Pulsar CTRL+ALT+SUPR y cerrar el programa "winsystem".

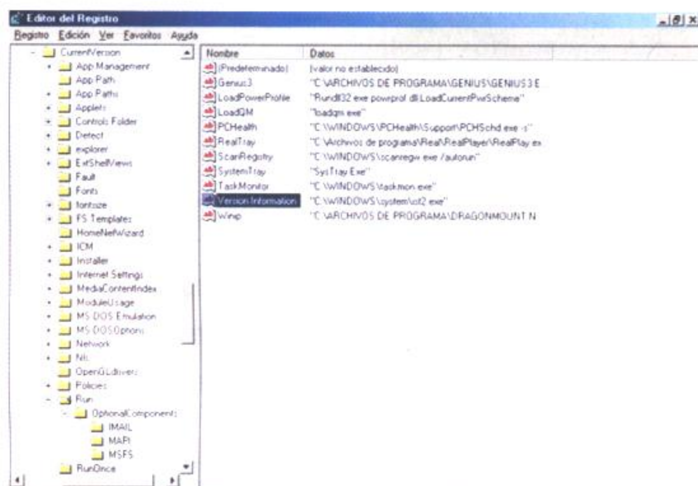
3º- Vamos a la carpeta C:\Windows\System y borramos los archivos "ist2.exe" y "windowskj.log"

4º- Pulsar INICIO ' EJECUTAR y escribimos "regedit" para entrar en el registro del sistema.

5º- Seguimos la siguiente ruta: HKEY_LOCAL_MACHINE ' Software ' Microsoft ' Windows ' CurrentVersion ' Run.

6º- Pinchamos sobre "Version Information" y pulsamos la tecla SUPR para borrar la entrada, nos saldrá un mensaje de confirmación donde deberemos aceptar.

7º- Vaciamos la papelera de reciclaje y reiniciamos el ordenador para comprobar que no queda ningún rastro.



Captura de pantalla de la localización del SKLOG en el registro.

Datos a tener en cuenta:

Un servidor de una red local almacena una serie de logs, indicando que usuario se ha conectado, desde que ordenador, la fecha y la hora y hasta que programas ha utilizado... Piensa que, si aparece registrado que se ha conectado desde un ordenador cercano a ti el administrador a una hora en la que este no esta trabajando o cuando solo tu estés en el trabajo, puede levantar sospechas, y si haces alguna faena es más que probable que lo investiguen.

Es conveniente averiguar cual es el tipo de servidor que utilizan y aprender algo sobre el, una información esencial es saber donde se almacenan los logs por si acaso metes la pata y tienes que borrar o modificar algo.

Problemas Frecuentes:

1º- El ordenador no tiene disquetera:

Lógico, se sabe que la mayor fuente de entrada de virus o de fugas de información en redes LAN se realiza por medio de disqueteras, el administrador ha optado por suprimirlas para evitarse problemas. Entonces debemos instalar una, solo tenemos que abrir la tapa del ordenador e instalar el cable de datos donde se muestra en la imagen (teniendo en cuenta que la línea roja debe coincidir con el "1" que estará grabado en el zócalo correspondiente, aunque... últimamente los cables vienen con posición), después cogemos uno de los cables de corriente con el conector más estrecho y se lo conectamos... y ya tenemos la disquetera conectada.



Aquí vemos como un ejemplo de como pueden estar colocados los conectores del disco duro, unidades de CD, etc. y de la disquetera, el conector de la disquetera es el mas estrecho de los tres.

2º- No se puede abrir la tapa, tiene un candado.

Suele pasar... de todas maneras fíjate en el candado para saber si es de cerradura o de combinación, tanto unos como otros suelen ser pequeños candados y muy poco seguros. Los de cerradura se abren fácilmente con una horquilla (la primera vez que lo intente tarde media hora, la segunda cinco minutos...), solo consiste en insistir hasta que se abra. Los de combinación solamente se abrirán si consigues dar con la combinación correcta, no obstante como suelen ser combinaciones de tres ruedas hay varias técnicas que te pueden facilitar el trabajo, la mas frecuente es probar con la numeración de la velocidad del equipo, la memoria RAM, alguna agrupación de tres números del serial del equipo.... a fin de cuentas el administrador se curara en salud por si algún día se le olvida la clave... y, en el peor de los casos tienes 1.000 combinaciones posibles, con tiempo y paciencia la encontraras...

3º- Una vez instalada la disquetera el PC no la reconoce.

Eso significa que esta desactivada de la BIOS, debemos activarla de la siguiente manera: Arrancamos al ordenador y mientras hace el test. de memoria pulsamos la tecla SUPR para entrar en la BIOS, nos saldrá una pantalla azul con varias opciones, elegimos "STANDARD CMOS SETUP", se nos abre otra pantalla con varias secciones, buscamos una llamada "DRIVE A" a cuyo lado veremos que pone "NONE", debemos pulsar las teclas REPAG y AVPAG, hasta que nos salga algo aproximadamente como esto: "1.44 Mb 3,5 In.", entonces debemos pulsar ESC para volver a la pantalla principal y escoger la opción "SAVE & EXIT SETUP", el ordenador se reiniciará y, al arrancar, veremos como la disquetera funciona correctamente.

```
ROM PCI/ISA BIOS (2A4IBS29)
STANDARD CMOS SETUP
AWARD SOFTWARE, INC.

Date (mm:dd:yy) : Sat, May  2 1998
Time (hh:mm:ss) : 19 : 54 : 53

HARD DISKS          TYPE   SIZE   CYLS HEAD PRECOMP LANDZ SECTOR  MODE
Primary Master    : User    420    986   16   65535   985     52 NORMAL
Primary Slave     : None      0      0    0       0     0      0 ------
Secondary Master  : None      0      0    0       0     0      0 ------
Secondary Slave   : None      0      0    0       0     0      0 ------

Drive A : 1.44M, 3.5 in.
Drive B : None                            Base Memory:    640K
                                      Extended Memory:  23552K
Video   : EGA/VGA                        Other Memory:    384K
Halt On : All Errors
                                         Total Memory:  24576K

ESC : Quit          ↑ ↓ →     : Select Item      PU/PD/+/- : Modify
F1  : Help          (Shift)F2 : Change Color
```

Captura de pantalla de la localización del SKLOG en el registro.

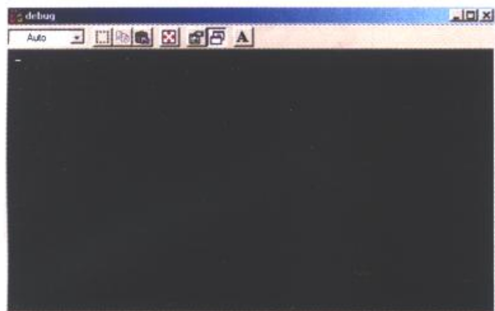
4º- Al entrar en la BIOS me pide una clave.

Síntoma de que el administrador ha protegido la BIOS con clave, para desprotegerlo hay programas concretos pero como no tenemos como ejecutarlos (todavía no tenemos disquetera para introducirlos) podemos quitar el password de las siguientes maneras:
-Vamos a INICIO ' EJECUTAR y escribimos "debug", con lo que se nos abrirá una ventana de MS-DOS donde escribiremos lo siguiente:
o 70 17
o 71 ff
q
Lo que hace este pequeño código es restablecer los valores opcionales de la BIOS.
-Si este truco no funcionase siempre queda la opción de resetearla "a mano" que consiste en abrir el equipo, quitar la pila de botón que esta alojada en la placa base, esperar un poco y volver a colocarla.

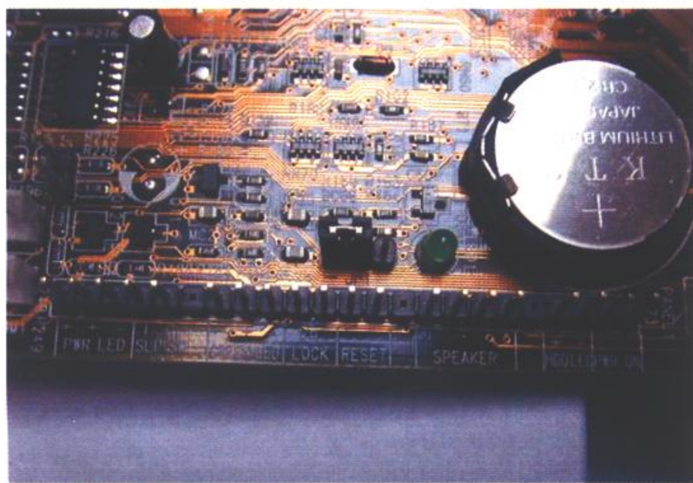


Una vez que...

Una vez que eliminas la clave no puedes averiguar cual tenia para volver a dejarla como estaba.



Captura de pantalla del programa Debug.



Vista de la pila de la placa base

5º- El SKLOG me pide el archivo "msvbvm60.dll".

Este archivo es una librería de Visual Basic, si te lo pide es porque no esta instalada en ese equipo, para instalarla debes localizarla (donde hayas descargado el SKLOG es probable que la tengan), descargártela y copiarla en el directorio c:/windows/system. Una vez lo hayas hecho el programa funcionara correctamente.

6º- Intento borrar el archivo "ist2.exe" pero no me deja, me dice que esta en uso.

No has cerrado el programa, pulsa CTRL+ALT+SUPR y ciérralo antes de eliminarlos.

Este es un pequeño ejemplo de como con un poco de ingenio y unos básicos conocimientos de hardware, así como de algún que otro sencillo programa, podemos entrar en redes que, a simple vista, parecen muy protegidas. Ahora debemos recordar que esto solo lo hacemos con una simple disquetera de 3 ½ , ¿has pensado que se podría llegar a hacer con una unidad de CD-ROM?, ¿o con un dispositivo USB como esas memorias flash que se venden ahora que son como un llavero?... Dejo estos retos para tu imaginación y tu ingenio.





SERVIDOR DE HXC MODO DE EMPLEO

- Hack x Crack ha habilitado un servidor para que puedas realizar las prácticas de hacking.

- Actualmente tiene el BUG del Code / Decode y lo dejaremos así por un tiempo (bastante tiempo ;) Nuestra intención es ir habilitando servidores a medida que os enseñemos distintos tipos de Hack, pero por el momento con un Servidor tendremos que ir tirando (la economía no da para mas).

- En el Servidor corre un Windows 2000 Advanced Server con el IIS de Servidor Web y está en la IP 80.36.230.235.

- El Servidor tiene tres unidades:
* La unidad c: --> Con 2GB
* La unidad d: --> Con 35GB y Raíz del Sistema
* La unidad e: --> CD-ROM

Nota: Raíz del Servidor, significa que el Windows Advanced Server está instalado en esa unidad (la unidad d:) y concretamente en el directorio por defecto \winnt\ Por lo tanto, la raíz del sistema está en d:\winnt\

- El IIS, Internet Information Server, es el Servidor de páginas Web y tiene su raíz en d:\inetpub (el directorio por defecto)

Nota: Para quien nunca ha tenido instalado el IIS, le será extraño tanto el nombre de esta carpeta (d:\inetpub) cómo su contenido. Pero bueno, un día de estos os enseñaremos a instalar vuestro propio Servidor Web y detallaremos su funcionamiento.

De momento, lo único que hay que saber es que cuando TÚ pongas nuestra IP (la IP de nuestro servidor) en tu navegador, lo que estás haciendo realmente es ir al directorio d:\Inetpub\wwwroot\ y leer un archivo llamado default.htm.

Nota: Como curiosidad, te diremos que APACHE es otro Servidor de páginas Web (seguro que has oído hablar de él). Si tuviésemos instalado el apache, cuando pusieses nuestra IP en TU navegador, accederías a un directorio raíz del Apache (donde se hubiese instalado) e intentarías leer una página llamada index.html

Explicamos esto porque la mayoría, seguro que piensa en un Servidor Web como en algo extraño que no saben ni donde está ni como se accede. Bueno, pues ya sabes dónde se encuentran la mayoría de IIS (en \Inetpub\) y cuál es la página por defecto (\Inetpub\wwwroot\default.htm). Y ahora, piensa un poco... ... ¿Cuál es uno de los objetivos de un hacker que quiere decirle al mundo que ha hackeado una Web? Pues está claro, el objetivo es cambiar (o sustituir) el archivo default.html por uno propio donde diga "hola, soy DIOS y he hackeado esta Web" (eso si es un lamer ;)

A partir de ese momento, cualquiera que acceda a ese servidor, verá el default.htm modificado para vergüenza del "site" hacheado. Esto es muy genérico pero os dará una idea de cómo funciona esto de hackear Webs ;)

- Cuando accedas a nuestro servidor mediante el CODE / DECODE BUG, crea un directorio con tu nombre (el que mas te guste, no nos des tu DNI) en la unidad d: a ser

posible (que tiene mas espacio libre) y a partir de ahora utiliza ese directorio para hacer tus prácticas. Ya sabes, subirnos programitas y practicar con ellos :)

Puedes crearte tu directorio donde quieras, no es necesario que sea en d:\mellamojuan. Tienes total libertad!!! Una idea es crearlo, por ejemplo, en d:\winnt\system32\default\mellamojuan (ya irás aprendiendo que cuanto mas oculto mejor :)

Es posiblemente la primera vez que tienes la oportunidad de investigar en un servidor como este sin cometer un delito (nosotros te dejamos y por lo tanto nadie te perseguirá). Aprovecha la oportunidad!!! e investiga mientras dure esta iniciativa (que esperamos dure largos años)

- En este momento tenemos mas de 600 carpetas de peña que, como tu, está practicando. Así que haznos caso y crea tu propia carpeta donde trabajar.



MUY IMPORTANTE...

MUY IMPORTANTE!!!!! Por favor, no borres archivos del Servidor si no sabes exactamente lo que estás haciendo ni borres las carpetas de los demás usuarios. Si haces eso, lo único que consigues es que tengamos que reparar el sistema servidor y, mientras tanto, ni tu ni nadie puede disfrutar de él :(Es una tontería intentar "romper" el Servidor, lo hemos puesto para que disfrute todo el mundo sin correr riesgos, para que todo el mundo pueda crearse su carpeta y practicar nuestros ejercicios. En el Servidor no hay ni Warez, ni Programas, ni claves, ni nada de nada que "robar", es un servidor limpio para TI, por lo tanto cuídalo un poquito y montaremos muchos más :)